

تكنولوجيا المعلومات في المجال الأمني



د/ أشرف السعيد أحمد



353-360285
A2861

تكنولوجيا المعلومات في المجال الأمني

مكتبة الإسكندرية
التزويد

دكتور

أشرف السيد أحمد

٢٠١٣

مكتبة خزانة
(شراء)

رقم التسجيل ١١٨٠٨٤

ملوان الكتاب: تكنولوجيا المعلومات في المجال الأمني

المؤلف: د. أشرف السعيد أحمد

الطبعة الأولى: ٢٠١٣

رقم الإيداع: ٣٠١٢/٢٣٥١٢

الترقيم الدولي: ٣ - ٠٢٩٠ - ٩٠ - ٩٧٧ - ٩٧٨

حقوق الطبع والنشر والاقتباس محفوظة للمؤلف ولا يسمح بإعادة نشر هذا العمل كاملاً

أو جزء منه إلا بإذن كتابي من المؤلف.

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿قُلْ هَلْ يَسْتَوِي الَّذِينَ يَعْلَمُونَ وَالَّذِينَ لَا

يَعْلَمُونَ إِنَّمَا يَتَذَكَّرُ أُولُو الْأَلْبَابِ﴾

(سورة الزمر، آية ٩)

صَدَقَ اللَّهُ الْعَظِيمُ



إهداء ..

إلى والدي جفظة الله.


إلى روح أُمي الطاهرة.

إلى شريكة عمري.

إلى بناتي العزيزات.

إلى جفيدة الخالي.

د. أشرف المعيد أحمد



تقديم

تشكل المعلومات دوراً حيوياً في حياة الأفراد والمجتمعات، فهي عنصر لا يفتنى عنه في أي نشاط نمارسه، فهي المادة الخام للبحوث العلمية، والمحك الرئيس لاتخاذ القرارات الصحيحة، وأضحى للمعلومة دور مهم وحيوي في إنتاج البشر وتدير الأمور، وتسهم في التنمية وتنعكس على الإنتاج، وتشكل السلوك القويم بما ينعكس على التقدم الإيجابي للفرد والجماعة والدولة.

فقد كان لوزارة الداخلية الحرص على مواكبة التقدم التكنولوجي وتوظيف تكنولوجيا المعلومات لخدمة الأغراض الأمنية، لدعم مقومات الأمن والاستقرار اللازم لتحقيق التنمية الشاملة، والتحول من الإدارة التقليدية إلى الإدارة الإلكترونية في مجال تكنولوجيا المعلومات الأمنية لتصبح من الركائز الأساسية لنجاح الحكومة الإلكترونية في مصر، وذلك من خلال توفير البيانات والمعلومات الدقيقة اللازمة لتأمين متطلبات المجتمع، ومواكبة التطور السريع والمذهل في تكنولوجيا الحاسبات الآلية والتطوير المستمر لآليات العمل الأمني بما يضمن الارتقاء بمستوى أداء الأجهزة الشرطية، باستخدام التقنيات المعلوماتية المتقدمة وتوفير المعلومات والبيانات القادرة على التعامل مع متغيرات الأحداث، ولقد أثر التطور السريع لتكنولوجيا المعلومات تأثيراً كبيراً وبالفأ في واقع العمل الأمني.

وسنتناول في هذا المؤلف موضوع تكنولوجيا المعلومات في المجال الأمني من خلال خمسة فصول،

الفصل الأول بعنوان: تكنولوجيا المعلومات وسنتناول من خلاله ماهية التكنولوجيا وخصائصها، ومفهوم المعلومات، ومفهوم تكنولوجيا المعلومات، وأنواع نظم المعلومات.

الفصل الثاني بعنوان: تكنولوجيا المعلومات الأمنية، وسنتناول من خلاله نشأة

نظام المعلومات في وزارة الداخلية، والتخطيط الاستراتيجي لتطوير نظم المعلومات بوزارة الداخلية، ومقومات بناء تكنولوجيا المعلومات الأمنية، وأهداف تكنولوجيا المعلومات الأمنية، وخصائص ومميزات المعلومات الأمنية، ومعايير جودة المعلومات الأمنية، تكنولوجيا المعلومات وصنع القرار الأمني، ومدى الحاجة لتكنولوجيا المعلومات في العمل الأمني.

الفصل الثالث بعنوان: استراتيجية أمن المعلومات، وسنتناول من خلاله مفهوم أمن المعلومات، ومفهوم الاستراتيجية، ومحل الحماية، والمخاطر المحتملة، وأهم أساليب تأمين قواعد البيانات.

الفصل الرابع بعنوان: تكنولوجيا المعلومات الأمنية والحكومة الإلكترونية، وسنتناول من خلاله مفهوم الحكومة الإلكترونية، تطبيقات وزارة الداخلية المصرية في مجال الحكومة الإلكترونية، وتكنولوجيا المعلومات الأمنية في مجال تيسير وتبسيط إجراءات حصول المواطنين على الخدمات الأمنية الجماهيرية.

الفصل الخامس بعنوان: دور التقنيات الحديثة في تطوير تكنولوجيا المعلومات الأمنية، وسنتناول من خلاله مفهوم التقنية البيومترية، وبصمة الإصبع، البصمة الوراثية.

ونأمل الله أن تكون قد وفقتنا في المساهمة ولو بشكل بسيط في عرض المعلومات الأساسية، التي تساعد الباحثين والمهتمين بمجال تكنولوجيا المعلومات الأمنية لواقعة عصر تكنولوجيا المعلومات.

المؤلف



الفصل الأول

تكنولوجيا المعلومات

الفصل الأول تكنولوجيا المعلومات

تمهيد:

إن فيض المعلومات الذى يواجه الأمم والشعوب أصبح التنبض والعصب لجهود التنمية والتحديث؛ حيث يغطى كل مجالات الحياة المعاصرة من عملية واقتصادية واجتماعية وتعليمية وثقافية ودينية، وأضحى للمعلومة دور مهم وحيوى فى نتاج البشر وتدير الأمور، وأصبح يقاس بمدى التقدم فى أية مهنة أو دولة أو منظمة أو فرد بما يتوافر لدى كل منهم من مستودع لا يتناقص من معلومات، وتشكل ذاكرة حية للمعارف والخبرات، وتسهم فى التنمية وتنعكس على الإنتاج، وتشكل السلوك القويم بما ينعكس على التقدم الإيجابى للفرد والجماعة والدولة. فالمعلومات تتطور بمعدلات سريعة بما يجعلها فى حالة تشكيل وتعديل على الدوام، وتكنولوجيا المعلومات تعمل على تحسين كفاءة المنظمات وفعاليتها.

وهى شئ ما تقدم، سنتناول هذا الموضوع على النحو الآتى :

أولاً: ماهية التكنولوجيا وخصائصها.

ثانياً: مفهوم المعلومات.

ثالثاً: مفهوم تكنولوجيا المعلومات.

رابعاً: أنواع نظم المعلومات.

أولاً - ماهية التكنولوجيا وخصائصها :

يعتبر لفظ التكنولوجيا من أكثر المفاهيم المتداولة للاستخدام فى الوقت المعاصر، من قبل الفرد العادى والمتخصص، فهو مفهوم متعدد الجوانب والأبعاد ولا يوجد اتفاق بين المفكرين على تعريف واحد لها، ولكنه لا يخرج عن الإطار الذى يرى أنها مجرد تنويع للعقل البشرى الذى يسعى للسيطرة على الطبيعة وفق ما يخدم مصالحه، فهى نوع من المعرفة التى من الممكن اكتسابها ونقلها وتطويرها وتطبيقها بواسطة أفراد مؤهلين ومنظمين فى هيئات وكيانات ومؤسسات مختلفة.

كلمة تكنولوجيا (Technology) هى كلمة يونانية تتكون من شقين الأول (Techno) ويعنى فن الصناعة أو التشغيل، والثانى (Logo) ويعنى علم أو منهج أى أن كلمة تكنولوجيا فى معناها اللغوى تعنى «العلم التطبيقى للتواحي الصناعية». هناك من يرى أن «التكنولوجيا ببساطة هى أسلوب أداء ويتضمن هيكلها مزيجاً مركباً متفاعلاً من تجهيزات آلية، وعمالة، وطرق عمل تؤلف بين التجهيزات والعمالة فى إجراءات أداء بأسلوب محدد لإنتاج أو تقديم سلعة أو خدمة أو أكثر»^(١). ورأى آخر يرى أنها بمثابة وعاء يجمع بين جانبى العلم والفن؛ حيث يتمثل جانب العلم فى الاعتماد على نتائج الأبحاث العلمية فى التطبيقات التكنولوجية بينما يتمثل جانب الفن فى قدرة الإنسان على التحكم فى تلك التطبيقات ووضع مجموعة القيم التى تضمن استخدام تلك التكنولوجيا بما يحقق خدمة المجتمع بصورة جيدة. وهناك من عرفها بأنها «عبارة عن أشياء مادية، تشمل المنتجات والأدوات والأجهزة المستخدمة فى الإنتاج - الأنشطة أو العمليات - وهى تشمل طرق وأساليب الإنتاج، والمعرفة اللازمة لتطوير واستعمال المعدات والأدوات والأساليب للحصول على مخرجات محددة». ورأى آخر يرى أنها

(١) أحمد سيد مصطفى، إدارة الإنتاج والعمليات فى الصناعة والخدمات، مكتبة الأنجلو المصرية، الطبعة الثالثة، القاهرة، ١٩٩٧م، ص ٨٠.

«عملية تاريخية تعكس التفاعل بين الإنسان وإدراكه للبيئة»⁽¹⁾. ويرجع السبب فى عدم تحديد مفهوم واحد للتكنولوجيا، إلى اختلاف مستويات التحليل التى اعتمد عليها المفكرون فى دراستهم للعلاقة بين التكنولوجيا والتنظيم. فمنهم من اهتم بدراسة التكنولوجيا على مستوى المنظمة، وهناك من اهتم بدراسة التكنولوجيا على مستوى مجموعات العمل داخل المنظمة وهناك فريق ثالث اهتم بدراسة التكنولوجيا على مستوى الأفراد⁽²⁾.

والتكنولوجيا هى نوع من المعرفة التى من الممكن اكتسابها ونقلها وتطويرها وتطبيقها، وتتطوى على درجة كبيرة وعالية عن التخصص، مما يسهل عملية اكتسابها أو تطبيقها، فهى ليست مجرد الأداة أو الوسيلة التى يستخدمها الإنسان فى حل مشاكله والتحكم فى بيئته، بل إنها تتسع لتشمل الظروف الاجتماعية التى أفرزت هذه الأداة، وكذلك الجوانب المختلفة للسلوك الاجتماعى فيما يخص تطبيقاته.

والتكنولوجيا هى عنصر ذو ثلاثة أبعاد،

- ١- البعد الفنى وهو متمثل فى العلم والمعرفة المتاحة.
- ٢- البعد التنظيمى والمتمثل فى توفير كافة احتياجات المجتمع من سلع وخدمات كما تساعد الإنسان على التغلب على المشاكل والصعوبات التى تواجهه.
- ٣- البعد التطبيقى والمتمثل فى قدرة الإنسان على الاستفادة من المعرفة المتاحة، وهى تتسم بالديناميكية والتطور المستمر، وتلعب دوراً أساسياً فى تحقيق التنمية الشاملة للمجتمع.

(1) Horrington Jonk Organization Structure And Information Technology, New York Prentice Hall International, 1991,P31.

(2) Yadav,D.S : Foundations Of Information Technology-3 rd ed, New age international limited publishers ,2006,P204.



خصائص التكنولوجيا:

١- التكنولوجيا علم مستقل له أصوله وأهدافه ونظرياته، ولا يتم فصل لفظ التكنولوجيا عن العلم، فلا يتصور أن تكون هناك تكنولوجيا إن لم ترافق مع ثورة علمية^(١).

٢- التكنولوجيا علم تطبيقي يسعى لتطبيق المعرفة.

٣- التكنولوجيا عملية تمس حياة الأفراد، وتعكس حضارة الشعوب، كما أنها الذاكرة الحية لهذا الشعب في زمن معين، والتطور البشري مرتبط بتطور التكنولوجيا.

٤- التكنولوجيا عملية شاملة لجميع العمليات الخاصة بالتصميم والتطوير، وهي تعنى بخطوات الحصول على الخدمة من المنظمات العامة، وتدفق العمل الذي يتم من خلال إعداد المستندات والملفات إلكترونياً داخل المنظمة، والهدف الرئيسي لتحسين الإجراءات إلكترونياً هو تقليل وإزالة هفاقد العمليات وتبسيط العمل وتوفير تغذية مرتدة من العملية، وخفض فترة العمل وتقليل الأخطاء في أداء الخدمة^(٢).

٥- التكنولوجيا هادفة، تهدف للوصول إلى حل المشكلات.

٦- التكنولوجيا متطورة ذاتياً، وتتسم بالرونة المستمرة في عمليات المراجعة ومدى قابليتها للتعديل والتجديد والتطوير فيها.

(1) Oliver. B.C. Chapman, R.J. French, C.S: Data processing And Information Technology -8 ed, DP Publications, Reviser, 1990, P154.

(2) Lucas, Henry C : Information Technology For Management -7 th ed (Boston :Irwin / McGraw -Hill, 2000) P122.

ثانياً - مفهوم المعلومات :

المعلومات هي ناتج تشغيل البيانات، وهي التي تعطى للبيانات معنى، وهي تزودنا بالأسس التي تقوم عليها القرارات⁽¹⁾. وهي تجميع بيانات خام وتنظيمها بواسطة التصنيف والمقارنة وتفسيرها وتقديمها للاستخدام بعد التفهم العميق؛ حيث يؤدي ذلك إلى بزوغ المعرفة.

وهناك علاقة وثيقة بين المعلومات والمعرفة، فالمعلومات تزيد رصيد الإنسان من المعرفة، وإذا لم تقم المعلومات بهذه المهمة فلا توصف بأنها معلومات، والمعرفة حصيلة أورصيد خبرات ومعلومات وتجارب ودراسة طويلة يملكها شخص معين مادي أو معنوي، وهي تختلف من شخص إلى آخر باختلاف المعلومات التي حصل عليها والتجارب التي خاضها والبيئة التي يعيش فيها، كما تختلف بالنسبة للفرد من وقت إلى آخر طبقاً لتلك الحصيلة والتي - غالباً - تزداد مع الزمن⁽²⁾.

مصادر المعلومات :

يتميز الإنسان بفضيلة العقل التي حباه الله إياها والتي تميزه عن كل المخلوقات، ومن ثم فإن المعلومات هي أداة الوصول إلى المعارف والمخترعات في كافة المجالات لتطوير الحياة، ويتم جمع المعلومات لتواكب المعرفة لمواجهة المتطلبات الحالية أو المستقبلية، ذلك يمثل الدافع لجمع المعلومات، فهي لا تجمع بهدف جمع المعلومات، ولكن لتحقيق أهداف شخصية لمن قام بجمعها أو لتحقيق أهداف المنظمة، ومهما تنوعت وتعددت المعلومات فإنه يمكن الحصول عليها من مصادر داخلية أو مصادر خارجية⁽³⁾.

(1) K. Samuelson and H. Borko and G.X.Aney : Information System And Network Amsterdam : North Holand Publishing Co.,1977).P47.

(2) Williams, Brian K, Sawyer, Stacey C : Using Information Technology,4 th ed,Boston: McGraw -Hill,2001,p127.

(3) Lucas, Henry C : Information Technology ,op.cit.p135.

أ- المصادر الداخلية:

هي المعلومات التي يحصل عليها الفرد أو تتجمع لدى المنظمة نتيجة للتصرفات والتفاعلات الداخلية في المنظمة، وهي تتجمع لدى الفرد أو المنظمة من خلال الأرشفة الخاص بالمنظمة، أو نظام المعلومات بالمنظمة الذي يتضمن المكاتب والسجلات والتقارير والملفات والنشرات والدوريات ... إلخ، التي تصدرها إحدى الإدارات الشرطية، أو المعلومات الشفوية التي تتم من خلال قنوات الاتصال المختلفة، والمعلومات التي يتم الحصول عليها من التحريات أو من المتواجدين في محل الحادث.

ب- المصادر الخارجية:

هي المعلومات التي تتعلق بالمتغيرات الاقتصادية والسياسية والثقافية، والمصادر الخارجية تشمل المعلومات التي تأتي من مصادر خارج الفرد أو المنظمة، ولكنها ذات صلة أو تأثير على الفرد أو المنظمة مثل بيانات أو معلومات من النقابات المهنية أو الحالة السياسية أو الاجتماعية أو الأمنية أو بيانات عن منظمات مهنية أو الإحصاءات التي تصدرها الجهات المختلفة^(١).

وتتمثل أنواع مصادر المعلومات فيما يأتي:

١- مصادر المعلومات العملية:

وهي المعلومات التي تتعلق بأنشطة الفرد أو المنظمة العملية المختلفة، وذلك من خلال القنوات الرسمية الخاصة بالمنظمة وغير الرسمية، وتشمل جميع المعلومات التي تتعلق بهذا النشاط أو ذات الصلة به.

(١) محمد محمد الهادي، التطورات الحديثة لنظم المعلومات المبينة على الكمبيوتر، القاهرة، دار الشروق، ١٩٩٢م، ص ٧١.

٢ - المصادر العلمية:

وهي تتعلق بالمعلومات العلمية والتكنولوجية المتصلة بمجال نشاط الفرد أو المنظمة، ويمكن الحصول عليها من قاعدة البيانات الخاصة بالمنظمة أو المنظمات المتخصصة في تلك المجالات العلمية والتكنولوجية والفنية المتخصصة، كأكاديمية البحث العلمي والتكنولوجي ومراكز ومعاهد البحوث العلمية والفنية^(١).

٣ - المصادر الثقافية:

وهي المعلومات التي يحصل عليها الفرد أو المنظمة من وسائل الإعلام وأجهزة الثقافة، مثل الإذاعة، والتليفزيون وأبحاث المنظمات الثقافية المتنوعة والمكتبات العامة وما تصدره الدولة من نشرات.

٤ - المصادر الذاتية:

هي مجموع المعلومات التي يختزنها الإنسان في ذاكرته وما اكتسبه من خبرات ومعارف، من خلال التعليم وتعامله وتجاريه واختزنها في ذاكرته^(٢).

الشروط التي يجب مراعاتها عند جمع المعلومات:

إن جمع المعلومات ليس عملية مرسلة، وإنما يجب أن تحكمها قواعد حتى لا تفقد قيمتها وتتفق الجهود في سبيل الحصول على معلومات أقل أهمية أو تؤدي إلى تجميع أكبر قدر من المعلومات، مما يقلل من كفاءة النظام لذلك كان من الضروري التعرض لبعض القواعد التي تعمل على توفير المعلومات الضرورية والأساسية لتحقيق أهداف

(١) عصمت عبد الله الشيخ : دور نظم وتكنولوجيا المعلومات في تيسير وفاعلية العمل الإداري، دار النهضة العربية، ١٩٩٠، ص ٤٥.

(٢) طارق إبراهيم الدسوقي : الأمن المعلوماتي والنظام القانوني لعملية المعلومات، القاهرة، دار اللمعة الجديدة للنشر، ٢٠٠٩، ص ٢٧.



النظام عند جمع المعلومات من مصادر خارجية ومنها:

١ - الارتباط بالموضوع أو نشاط المنظمة،

أن تكون هذه المعلومات مرتبطة بالموضوع الذي منيتم جمع المعلومات من أجله وأن تكون متصلة اتصالاً مباشراً بأنشطة وأهداف المنظمة ومؤثرة على هذا النشاط، وأن يتحاشى جمع معلومات هامشية أو ثانوية، بل يجب التركيز على المعلومات الأساسية الضرورية لتحقيق الهدف أو التأثير ذاته على مجالات الأنشطة المختلفة.

٢ - أن تكون المعلومات حديثة؛

يراعى أن تكون المعلومات التي يقوم بجمعها الفرد أو المنظمة تمثل أحدث المعلومات في مجال النشاط، إلا في حالة الأبحاث أو التقارير التي توضح التطور التاريخي للظاهرة أو الحدث.

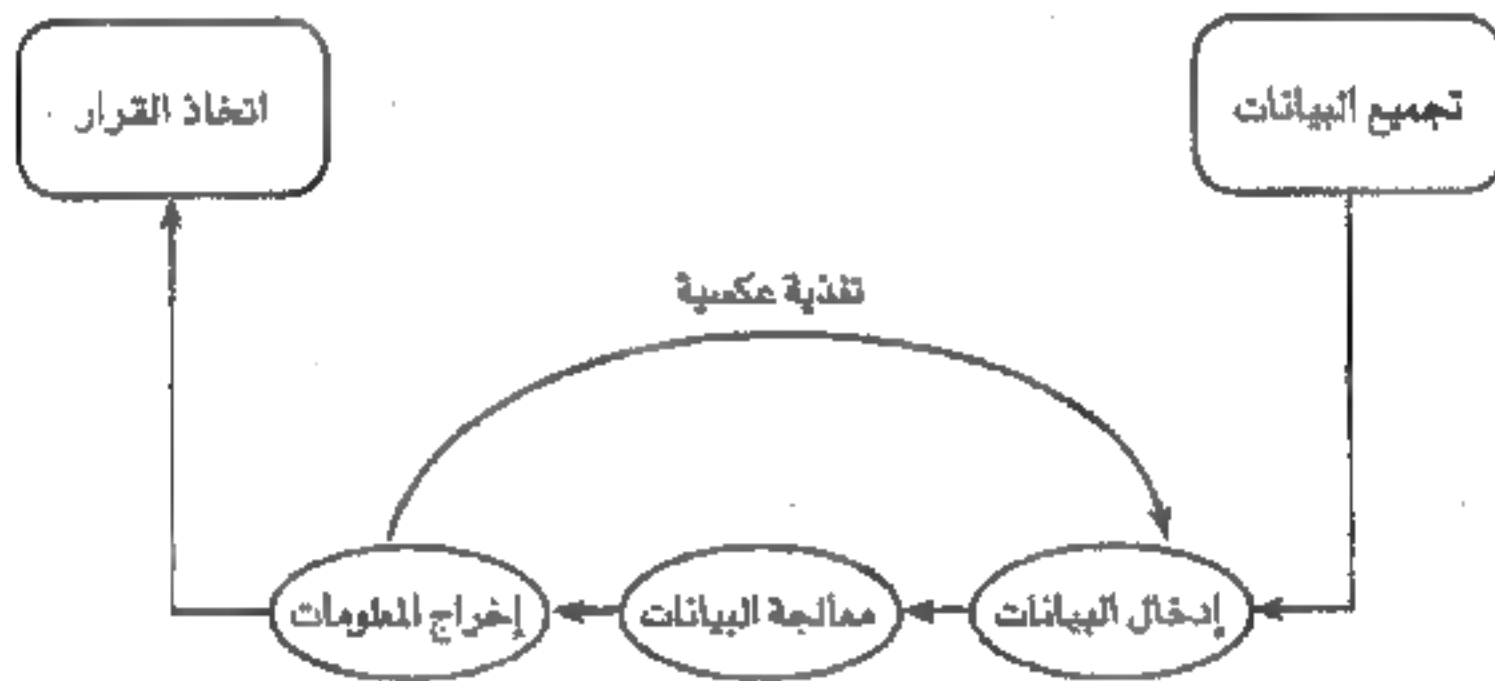
٣ - الثقة في مصادر المعلومات؛

يراعى أن تكون المصادر التي تجمع المعلومات موضع ثقة من الناحية العلمية أو البحثية، وأن تكون مصادرها محددة ودقيقة، حتى تكون ذات قيمة. بالإضافة إلى ذلك فإن المعلومات قد تكون متوفرة في أكثر من مصدر أو في أكثر من موقع بالنسبة للمصدر الواحد؛ حيث إن كثرة المصادر ووفرتها وتعدد الأماكن بالنسبة للمصدر الواحد قد تجعل من المستحيل تغطيتها كلها، ومتابعة التملورات والتحديث في كل منها، وفي هذه الحالة يجب وضع أولويات بالنسبة لهذه المصادر وتعدد الأماكن بالنسبة للمصدر الواحد^(١)، وأن يكون أساس المفاضلة هو التعمق وحداثة المعلومات بالإضافة إلى مدى شمول المعلومات وتغطيتها لنوع المجال أو النشاط، أو مجال البحث، ويستلزم

(1) Yadav, D.S, op. cit, p215.

وجود المعلومات توفر وعاء يحتويها وهو ما يطلق عليه بالوثيقة أو بمصدر المعلومات بأشكالها وأحجامها المختلفة، والمعلومات أبعاد أهمها⁽¹⁾:

- ١- الكمية : والتي تقاس بعدد الوثائق، الصفحات، الكلمات، الرسوم، والصور.
- ٢- المحتويات : وهي معنى المعلومات.
- ٣- البنية : وهي تشكل المعلومات والعلاقة المنطقية بين نصوصها وعناصرها.
- ٤- اللغة : وهي الرموز والحروف والأرقام التي يعبر بواسطتها عن الأفكار.
- ٥- الجودة : وهي أن تكون المعلومات كاملة وصحيحة وذات فائدة.
- ٦- العمر : وهو الفترة الزمنية التي تكون فيها المعلومات ذات قيمة.



شكل رقم (١-١) نموذج مبسط لنظام المعلومات

(1) Weisman, H.M : Information Systems Services And Centers, London: John Wiley, 1972, p13.

ثالثاً - مفهوم تكنولوجيا المعلومات :

يعتبر مفهوم تكنولوجيا المعلومات من أكثر المفاهيم استخداماً في الدراسات المعاصرة فهو مفهوم متعدد الجوانب والأبعاد، وهي أحدث مقررات التطور التكنولوجي، وأدى التطور التكنولوجي المتمثل في الاتصالات إلى إلغاء الحواجز بين الدول، ولقد تباينت اتجاهات الباحثين في دراستهم لتكنولوجيا المعلومات، فهناك من اهتم بالمتغيرات والأبعاد الفنية وعرف تكنولوجيا المعلومات باعتبارها أدوات وتطبيقات هندسية تقوم بتنفيذ ما تلقاه من أوامر وتعليمات^(١)، مع إبراز دور التكنولوجيا في الحصول على المعلومات؛ حيث صُرف البعض تكنولوجيا المعلومات «أنها تشمل جميع أشكال التكنولوجيا التي تمكن الأفراد من خلق ومعالجة المعلومات».

ونرى أن هذا التعريف خلط بين مفهومي البيانات والمعلومات؛ حيث تستخدم التكنولوجيا في معالجة البيانات، والتي تعتبر بمثابة المادة الخام، للحصول على المعلومات، التي تمثل المنتج النهائي.

وهذا ما دفع البعض إلى تعريف تكنولوجيا المعلومات بأنها «تطبيق للتكنولوجيا الإلكترونية ومنها الحاسب الآلي والأقمار الصناعية وغيرها من التكنولوجيات المتقدمة لإنتاج المعلومات التناظرية والرقمية وتخزينها واسترجاعها وتوزيعها ونقلها من مكان إلى آخر»^(٢)، وتتميز التعريفات السابقة بأنها أوضحت أن معالجة المعلومات تتم بشكل إلكتروني أو باستخدام التكنولوجيات الإلكترونية.

وهناك من يرى أن تكنولوجيا المعلومات هي مزيج من تكنولوجيا الاتصالات

(1) Gershenfeld, Neil: The Physics Of Information Technology, Cambridge, New York : Cambridge University Press ,2000 ,p95.

(٢) حسن عماد مكاوي : تكنولوجيا الاتصال الحديثة في عصر المعلومات، الطبعة الأولى، القاهرة، الدار المصرية اللبنانية، ١٩٩٣، ص ٧٩.

وتكنولوجيا الحاسبات الإلكترونية وقد أصبحت تكنولوجيا المعلومات الآن هي الزاد الرئيسى للتطوير التكنولوجى^(١)، وهناك من يُعرف تكنولوجيا المعلومات بأنها حصيلة تزاوج وتفاعل ثلاث تكنولوجيات متمثلة فى: تكنولوجيا الحاسبات؛ وذلك بما تقدمه من حواسيب فائقة القدرة وتجهيزات متنوعة تيسر للإنسان إمكانية التعاوم معها، تكنولوجيا البرمجيات؛ والتي تشمل نظم تصميم وتنفيذ وإدارة قواعد البيانات ونظم استخدام الحاسبات فى التطبيقات المختلفة ونظم التخطيط وتنفيذ واختيار البرمجيات بمساعدة الحاسب، وأخيراً تكنولوجيا الاتصالات؛ بما تقدمه من أساليب وتقنيات تساعد على ربط الحاسبات ونظم المعلومات بعضها ببعض فى أنظمة متكاملة على كافة المستويات» ونرى أن هذا الرأى يركز على إبراز الأنواع التكنولوجية المختلفة التى ساهمت فى ظهور وانتشار تكنولوجيا المعلومات، ولم يهتم بالأهداف التى تسعى هذه التكنولوجيا إلى تحقيقها أو الأنشطة التى يتم من خلالها تحقيق تلك الأهداف؛ حيث يرى أن تكنولوجيا المعلومات هى مزيج بين ثلاث تكنولوجيات متمثلة فى تكنولوجيا الحاسبات الرقنية، وتكنولوجيا تخزين البيانات وتكنولوجيا الإشارات الرقمية والاتصال عن بُعد^(٢)، وهناك من يرى أن مصطلح تكنولوجيا المعلومات يشمل جميع أنواع التكنولوجيات المستخدمة فى جمع ومعالجة أو تبادل واستخدام المعلومات بأشكالها المختلفة^(٣)، وهو يركز على أجهزة الحاسبات والبرمجيات فقط؛ حيث يميل إلى استخدام الحاسبات الإلكترونية والبرمجيات لتحويل وتخزين، وحماية ومعالجة واسترجاع المعلومات من أى مكان وفى أى وقت، ونرى أن هذا التعريف يتسم بالعمومية الشديدة ومن الممكن أن ينطبق على أى

(١) أحمد سيد مصطفى: المفاهيم التكنولوجية على المؤتمر البشرى فى المنظمات العربية، ورقة عمل نشرت بمجلة أفاق اقتصادية، العدد ٧٣، مجلد ١٩، ١٩٨٩م، ص ٩.

(٢) عماد عبد الوهاب الصباغ: علم المعلومات، دار الثقافة للنشر والتوزيع، قطر، ٢٠٠٤م، ص ١٨٠.

(٣) E. Wainright Martin et al : Managing Information Technology : What Managers Need To Know?, (New Jersey : Prentice Hall , 1999).p 24.

نظام معالجة البيانات بما في ذلك النظم اليدوية أو التقليدية التي تعتمد على الأدوات والأجهزة ذات الإمكانيات المحدودة. وهناك من نظر إلى تكنولوجيا المعلومات على أنها نظام فرعي، يهتم بأجهزة الحاسب الآلي وأجهزة الاتصالات.

وتتمثل تكنولوجيا المعلومات في استخدام أجهزة الحاسبات للبرمجيات والاتصالات في إدخال وتشغيل وتخزين ونقل المعلومات، وهي تعتبر نتاج تزاوج وتفاعل ثلاث تكنولوجيا من أجل تحقيق هدف معين وهو توفير الوقت وسهولة في التنفيذ من خلال الآتي:

١ - تكنولوجيا الحاسبات:

وذلك بما تقدمه من حواسيب فائقة القدرة وتجهيزات متنوعة تيسر للإنسان إمكانية التماور معها، والسرعة في تنفيذ الأوامر والعمليات الحسابية والمنطقية والإمكانيات الهائلة للحفظ والاسترجاع وإعداد التقارير والإحصائيات^(١).

٢ - تكنولوجيا البرمجيات :

والتي تشتمل على نظم تصميم وتنفيذ وإدارة قواعد البيانات ونظم استخدام الحاسبات في التطبيقات المختلفة ونظم تخطيط وتنفيذ واختبار البرمجيات بمساعدة الحاسب.

٣ - تكنولوجيا الاتصالات :

وذلك بما تقدمه من أساليب وتقنيات تساعد على ربط الحاسبات ونظم المعلومات بعضها ببعض في أنظمة متكاملة على كافة المستويات. وسرعة نقل المعلومات والمشاركة في البيانات والأجهزة من خلال شبكات نقل المعلومات.

(١) على عبد الهادي معلوم، مفكرات في نظم المعلومات الحديثة على الكمبيوتر - المبادئ والتطبيقات، مركز التنمية الإدارية، جامعة الإسكندرية، ١٩٩٤م، ص ١١٧.

ولقد أحدثت تكنولوجيا المعلومات تأثيرات جوهرية في النظم الإدارية من أهمها:

١- تحقيق الاستخدام الأمثل للموارد البشرية والفنية والمادية المتاحة للمنظمة والعمل على تسميتها كما وكيفاً.

٢- خلق قنوات اتصال جديدة من خلال شبكات الحاسبات والاتصالات سواء على مستوى المنظمة أو على المستوى القومي أو العالمي مما مكن من زيادة سرعة تدفق ومعالجة وتبادل المعلومات وتطوير أساليب إدارية حديثة كالاتصالات والتفاوض وعقد الصفقات عن بُعد.

٣- مساعدة المديرين على التخلص من أعباء المهام الروتينية مما أتاح لهم إمكانية استخدام فائض في أوقاتهم للعمل في مجال التخطيط الاستراتيجي ورسم السياسات ولقد انعكس ذلك بشكل واضح في رفع كفاءة الإدارة العليا^(١).

٤- ساهمت في زيادة قدرة النظم الإدارية على التكيف السريع مع بيئة العمل الإداري، من خلال توفير وسائل اقتصادية فعالة لتخزين واسترجاع ومعالجة البيانات، وتقديمها إلى متخذ القرار في الوقت المناسب^(٢).

تعتبر تطبيقات تكنولوجيا المعلومات أكثر انتشاراً في المجالات الإدارية بالمقارنة مع المجالات الأخرى، فهي تؤثر مباشرة في نظم الاتصال واتخاذ القرارات.

(1) Lucas, Henry C, op. cit, p105.

(2) Fletcher, Keith : Marketing Management And Information Technology, New York: Prentice Hall, 1995,p42.

رابعاً - أنواع نظم المعلومات :

هناك العديد من أنواع نظم المعلومات لتلبية الاختلافات في حاجة القيادات إلى المعلومات في الجهة أو المنظمة، وهي تشمل نظم المعلومات التشغيلية، النظم المعرفية، ونظم تجهيز المكاتب آلياً، ونظم المعلومات الإدارية، ونظم دعم القرارات، ونظم دعم الإدارة العليا، والنظم الخبيرة^(١).

١ - نظم تشغيل البيانات :

يهدف هذا النوع من نظم المعلومات إلى خدمة المستويات التشغيلية داخل الجهة، ويعتمد على الحاسب الآلي لتسجيل البيانات الروتينية، وتتمتع نظم التشغيل بالآتي:

- رسم حدود المنظمة وبيئتها من خلال ربط جميع فروعها.
- تعد نظم المعلومات منتجة للمعلومات وإعدادها للاستخدام في الجهة أو إدارات أخرى.

٢ - النظم المعرفية :

تهدف تلك النظم إلى دعم العاملين بالجهة في مجال المعرفة والمعلومات من خلال ضمان وصول المعرفة والمعلومات بشكل متكامل داخل الجهة، وهي تعنى الإضافة العلمية والثقافية من مصدر أو أكثر؛ حيث تؤدي هذه النظم المعرفية إلى اتساع إدراك الإنسان فتجعله قادراً على معالجة أية مشكلة تواجهه في مجالات المعرفة التي تعلمها^(٢).

(1) O'Brien, James A : Management Information Systems, 3rd ed ,Chicago: Irwin, 1996, p119.

(٢) علاء عبد الرازق السالمى : نظم إدارة المعلومات، النوحة، قطر، المنظمة العربية للتنمية الإدارية، ٢٠٠٧م، ص ٢٢١.

٣ - نظم تجهيز المكاتب آلياً:

تعد تلك النظم نوعاً خاصاً من نظم تشغيل المعلومات والتي يمكن استخدامها في نطاق أعمال وأنشطة الإدارات والمكاتب، ويقصد بتجهيز المكاتب كل أنواع نظم الاتصالات الرسمية، وغير الرسمية، المتعلقة بتوصيل المعلومات المكتوبة، وغير المكتوبة من شخص إلى آخر سواء داخل الجهة أو خارجها، ومن أمثلة الأجهزة المستخدمة في تجهيز المكاتب البريد الإلكتروني، البريد الصوتي، شبكات الحاسب الآلي، اجتماعات الفيديو.

٤ - نظم المعلومات الإدارية:

هي مجموعة من النظم الفرعية التي يؤدي تفاعلها إلى إنتاج المعلومات التي تغطي الاحتياجات المختلفة للأنشطة الإدارية، وبتزايد حجم المعلومات التي تتعامل من خلالها نظم معلومات الجهات أصبحت نظم معالجة البيانات غير قادرة على توفير احتياجات متخذ القرار من معلومات واتجهت إلى الاعتماد على نظم المعلومات المبنية على الحاسب الآلي.

٥ - نظم دعم القرارات:

هي نظم معلومات تهدف إلى مساعدة المديرين والقيادات لاتخاذ قرارات غير متكررة، وتعتمد على نظم تشغيل المعلومات ونظم المعلومات الإدارية، ويتم تصميم نظم دعم القرارات استجابة للاحتياجات غير المخططة من المعلومات^(١).

٦ - نظم دعم الإدارة العليا:

هي تلك النظم التي يتم تصميمها لمساندة القيادة العليا التي لها تأثير ملموس على سياسات وخطط واستراتيجيات الجهة أو المنظمة، وتتعامل تلك النظم مع القرارات

(١) أحمد سيد مصطفى: المثير العربي في عالم متغير القاهرة، بدون ناشر، ص ١٢٨.

الفصل الأول - تكنولوجيا المعلومات

التي تلعب البيئة الخارجية دوراً ملموساً ومؤثراً عند اتخاذها، وهي قرارات ذات درجة عالية من عدم التأكد.

٧ - النظم الخبيرة:

تستخدم النظم الخبيرة لمساعدة متخذ القرار في التعامل مع القرارات غير الروتينية والتي لا يمكن التنبؤ بها، وتعتمد تلك النظم غير الروتينية على نتائج ما يسمى بالذكاء الاصطناعي؛ حيث تقوم تلك النظم على فكرة محاكاة عملية اتخاذ القرار التي يقوم بها المتخصص، وتتشكل العناصر الأساسية لبنية المعلومات من جزأين رئيسيين وهما:

أ - نظم الحاسبات الآلية:

هي تتضمن المكونات المادية والبرمجيات والبيانات والملفات والاتصال عن بُعد وهي تعد العنصر الرئيسي لتطبيقات النظم، وبالتالي فإن نجاح الجهة يتوقف على مقدرة تلك النظم على توفير الاحتياجات للجهة حالياً ومستقبلاً^(١).

ب - نظم التطبيقات الإدارية:

هي مجموعة من العمليات المنتظمة التي تعد المديرين بالمعلومات اللازمة لمساعدتهم في تنفيذ الأعمال واتخاذ القرارات، وتشمل بيانات الموارد البشرية والمادية التي يتوقف على تحقيق أهدافها^(٢).

(١) على فهمي: نظم دعم اتخاذ القرار والأنظمة الذكية، القاهرة، دار الكتب للنشر والتوزيع، القاهرة، ٢٠٠٦م، ص ٧١.

(2) Lucas, Henry C., op. cit, p92.



الفصل الثاني

تكنولوجيا المعلومات الأمنية

الفصل الثاني تكنولوجيا المعلومات الأمنية

تمهيد:

أصبحت فلسفة استخدام تكنولوجيا المعلومات الأمنية في مجالات الحياة المعاصرة علامة مميزة وضرورة عصرية لا غنى عنها، وهدف استراتيجي في إطار السياسة الأمنية المعاصرة، بغية تدعيم القيم الإنسانية والأخلاقية، واحترام القانون وسيادة الشرعية الدستورية، وصيانة حقوق الإنسان، وترسيخ قواعد العدالة الجنائية، والارتقاء بمستوى الخدمات الأمنية الجماهيرية، وباعتبارها النبض والعصب لجهود التنمية الاقتصادية والاجتماعية، والثقافية، والعلمية.

وفي ضوء ما تقدم، سنتناول هذا الموضوع على النحو الآتي :

- أولاً : نشأة نظام المعلومات في وزارة الداخلية.
- ثانياً : التخطيط الاستراتيجي لتطوير نظم المعلومات بوزارة الداخلية.
- ثالثاً : مقومات بناء تكنولوجيا المعلومات الأمنية.
- رابعاً : أهداف تكنولوجيا المعلومات الأمنية.
- خامساً : خصائص ومميزات المعلومات الأمنية.
- سادساً : معايير جودة المعلومات الأمنية.
- سابعاً : تكنولوجيا المعلومات وصنع القرار الأمني.
- ثامناً : مدى الحاجة لتكنولوجيا المعلومات في العمل الأمني.

أولاً - نشأة نظام المعلومات في وزارة الداخلية :

تعد وزارة الداخلية من أولى الوزارات التي تحرص على مواكبة التقدم التكنولوجي وتوظيف تكنولوجيا المعلومات لخدمة الأغراض الأمنية، لدعم مقومات الأمن والاستقرار اللازم لتحقيق التنمية الشاملة، من خلال توفير البيانات الحديثة والمعلومات الدقيقة اللازمة لتأمين متطلبات المجتمع، ومواكبة التطور السريع والمذهل في تكنولوجيا الحاسبات الآلية من خلال التطوير المستمر لآليات العمل الأمني بما يضمن الارتقاء بمستوى أداء الأجهزة الشرطية، باستخدام التقنيات المعلوماتية المتقدمة بتوفير المعلومات والبيانات القادرة على التعامل مع متغيرات الأحداث.

مركز الحاسبات الإلكترونية بوزارة الداخلية :

البداية كانت في ١٥ مايو ١٩٧٦ ، عندما أعطى السيد / ممدوح سالم رئيس الوزراء في ذلك الوقت إشارة البدء لعمل أول نظام حاسب آلي (Main Frame) بمركز الحاسبات الإلكترونية بوزارة الداخلية، وهو ثاني حاسب آلي في مصر ومنطقة الشرق الأوسط، وقد أنشئ لخدمة أغراض مراقبة الحدود والتسجيل الجنائي، وشملت شبكة الاتصال بهذا الحاسب عدد ١٨٠ نهاية طرفية تعمل عن بُعد بخطوط مؤجرة (Leased Line) تربط مصلحة الجوازات ومينائي القاهرة الجوى والإسكندرية البحرى (بالنسبة لنظام مراقبة الحدود) ومديريات أمن القاهرة، الإسكندرية، أسيوط بالنسبة لنظام (التسجيل الجنائي)، بلغت السعة القصوى لذاكرة هذا الحاسب ٢٥٦ كيلوبايت والسعة التخزينية للأقراص الصلبة ٢٥ ميجا بايت، وقد استمر العمل بهذا النظام حتى عام ١٩٨٤م^(١).

وكان هذا النظام يهدف إلى ما يلي :

- الكشف الفوري على المغادرين والقادمين عبر مطار القاهرة الجوى وميناء

(١) ندوة تكنولوجيا المعلومات الأمنية سنوات من التحديث والإنجاز، مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة، ٢٠٠١م، ص ١٢.

الإسكندرية البحري ومقارنة بياناتهم بقوائم المتنوعين بمصلحة وثائق السفر،
- تسجيل بيانات الأشخاص المطلوبين ومن لهم معلومات جنائية للاستفادة
بهذه المعلومات في حالات الاستعلام أو طلب معلومات لأغراض أعمال البحث
والتحري.

الإدارة العامة للمعلومات والتوثيق بوزارة الداخلية :

في عام ١٩٨١ صدر القرار الجمهوري رقم (٦٢٧) لسنة ١٩٨١م بإنشاء مراكز
معلومات بأجهزة الدولة ، وتبعه صدور القرار الوزاري رقم (٤٠٥) لسنة ١٩٨٢ بإنشاء
الإدارة العامة للمعلومات والتوثيق بوزارة الداخلية أكبر الأثر في تطوير وميكنة نظم العمل
بكافة جهات الوزارة، وخطت الوزارة خطوة مهمة في هذا المجال؛ حيث شكلت اللجنة
العليا لتنظيم المعلومات بالقرار الوزاري رقم (٨٨١٥) لسنة ١٩٩٢ والتي أوكل إليها مهمة
وضع الاستراتيجية والخطط والبرامج المحددة الأهداف ووسائل تحقيقها والمدى الزمني
اللازم للتنفيذ والمحدد بدقة وذلك لعمل منظومة معلومات متكاملة للوزارة تقوم على
عدة محاور وتشمل قواعد بيانات متكاملة على المستويين الجغرافي والتنوع في مجالات
مختلفة وتشمل، المعلومات الأمنية، المعلومات المالية، المعلومات الإدارية، العمليات (نظم
القيادة والسيطرة)، الأنشطة الخدمية للمواطنين^(١).

شبكة الإنترنت لوزارة الداخلية :

نظراً للتطور المعلوماتي السريع كان لوزارة الداخلية السبق في تطوير أسلوب العمل
باستخدام تقنيات شبكات الحاسبات الآلية، والقرار بإنشاء شبكة معلومات وزارة
الداخلية الموحدة الأثر الأكبر والفعال في تعظيم الأداء الأمني، وتطبيق منظومة الحكومة
الإلكترونية.

(١) للمزيد، راجع القرار الوزاري رقم (٤٠٥) لسنة ١٩٨٢ بشأن إنشاء الإدارة العامة للمعلومات والتوثيق والهيكل التنظيمي لها،
ونظرة العمل ومهام كل إدارة فرعية وقسم بها.

الفصل الثاني - تكنولوجيا المعلومات الأمنية

بتاريخ ٢٥ يناير ٢٠٠١م أُعطيت إشارة البدء لعمل شبكة الإنترنت التي تتيح انسياب المعلومات وتبادلها بين قطاعات وأجهزة الوزارة بأسلوب تقني متطور، وفي إطار من السرية وعدم القدرة على اختراقها من خارج الوزارة، بهدف رفع مستوى الأداء والتعامل بأسلوب عصري مع معطيات القرن الحادي والعشرين وكيفية الاستفادة المثلى منها للعبور على المعوقات الزمنية والنمطية الروتينية، وبما يتيح إمكانية اتخاذ القرار السليم المرتكز على قاعدة معلومات أمنية مؤمنة مدخلاتها ومخرجاتها^(١).

ثانياً - التخطيط الاستراتيجي لتطوير نظم المعلومات بوزارة الداخلية :

في ظل الاعتماد على تكنولوجيا المعلومات كان لا بد من وجود هدف استراتيجي تسعى الوزارة من أجل تحقيقه، من خلال تحقيق مجموعة أهداف أخرى فرعية، وتنفيذ مجموعة من الإجراءات لتحقيق الهدف الفرعي ومن أهم تلك الأهداف لتطوير نظم المعلومات بوزارة الداخلية تتمثل فيما يلي:

١- وضع خطة بعيدة المدى للمعلوماتية تتوافق مع خطة وزارة الداخلية الاستراتيجية وتلبي احتياجات الخطط الأمنية الأخرى.

٢- توفير المعلومات الأمنية المتكاملة على مستوى الجمهورية لكافة أجهزة البحث بمديريات الأمن والإدارات والمصالح والمنافذ وفروعها الجغرافية.

٣- ربط وتوحيد جميع أنظمة المعلومات بكافة جهات الوزارة بما يحقق تكامل نظم المعلومات الأمنية من خلال شبكة معلومات موحدة، مما يسهم في سهولة وسرعة تبادل المعلومات في إطار السرية وعدم القدرة على اختراقها، من خلال شبكة معلومات وزارة الداخلية.

(١) ندوة تكنولوجيا المعلومات الأمنية ستوات من التحديث والتجديد، مرجع سابق، ص ١٦.

٤- تطوير العمل بالأقسام والمراكز بإدخال أجهزة الحاسبات الآلية وربطها بقاعدة بيانات التسجيل الجنائي والمحكوم عليهم الهاربين من خلال شبكة معلومات وزارة الداخلية.

٥- تطوير العمل بأقسام الرقابة الجنائية واستحداث المنظومات الآلية للذكاء الاصطناعي ونظم الخبرة بما يسهم في دراسة الظواهر الإجرامية وإصدار الإحصائيات والتقارير بما يعزز القدرة على العمل الجماعي ووضع خطط التأمين والضبط لتكون متوافقة مع المواقف الأمنية المختلفة.

٦- الاعتماد على نظم الخرائط الجغرافية والتي تسهم في رصد البؤر الإجرامية والتفاصيل الطبوغرافية لداخل ومخارج تلك البؤر.

٧- دعم الدوريات الأمنية والأمنية الثابتة والمتحركة بأجهزة حاسبات مرتبطة بشبكة معلومات وزارة الداخلية لتحقيق الفحص الأمني بمحل الاستيقاف.

٨- العمل على إتاحة أكبر قدر من خدمات وزارة الداخلية الجماهيرية عبر شبكة الإنترنت الدولية لتسهيل على المواطنين الحصول على الخدمة.

٩- وضع البرامج التدريبية وتنمية الموارد البشرية من الضباط والأفراد والعاملين المدنيين في مجال استخدام الحاسبات الآلية.

ثالثاً - مقومات بناء تكنولوجيا المعلومات الأمنية:

واكبت مشروعات تكنولوجيا المعلومات الأمنية، أحدث ما توصلت إليه الثورة العلمية والتكنولوجية، من أجل خدمة أهداف التنمية، من خلال الآتي:

- بناء شبكة معلومات متطورة طبقاً لأحدث التقنيات الحديثة في وسائل الاتصال، لتطوير أساليب العمل والتشغيل بمختلف أجهزة الوزارة .

الفصل الثلثى - تكنولوجيا المعلومات النهائية

- بناء نظم معلومات تحقق التكامل بين أجهزة الوزارة على المستوى (النوعى - الجغرافى)، وتكفل معالجة المشاكل والمواقف الأمنية وإدارة الأزمات.
- بناء قواعد بيانات لكافة مجالات العمل بالوزارة (الأمنية - الخدمية - التعليمية - التدريبية - الإدارية - المالية).
- الاهتمام بإعداد كوادر مُدرّبة لرفع مستوى الأداء الشرطى وتدريب علوم نظم المعلومات بجميع الكليات والمعاهد الشرطية لجميع ضباط وأفراد الشرطة والعاملين المدنيين بالوزارة.

البنية الأساسية لشبكة الإنترنت لوزارة الداخلية:

تعد الإنترنت شبكة معلومات مبنية بتكنولوجيا الإنترنت ممتدة جغرافياً إلى كافة قطاعات الوزارة ومديريات الأمن والإدارات العامة والمصالح والمنافذ الحدودية وأقسام ومراكز الشرطة بجمهورية مصر العربية، وقوامها حاسبات رئيسية ذات سعات تخزين ضخمة بالمركز الرئيسى وحاسبات خادمة بجهات الوزارة محمل عليها مواقع (Web Sites) تلك الجهات، وقد تم ربط الحاسبات الخادمة بالحاسبات الرئيسية عبر شبكة اتصالات رقمية مستخدمة خطوط البنية التحتية للشبكة القومية للاتصالات، كما تم وضع مجموعة من القيود التأمينية للشبكة لفلقها تماماً لكافة الجهات والأفراد ويصرح فقط للجهات الشرطية بالدخول على مواقع الشبكة.

مكونات شبكة الإنترنت :

تتكون شبكة معلومات الوزارة (الإنترنت) من ثلاثة أجزاء رئيسية، هي :

١ - شبكة الاتصالات (Communication) :

فى بداية نشأة شبكة الإنترنت تم الاعتماد فى بناء شبكة الاتصالات على البنية الأساسية

التحتية للشبكة القومية للاتصالات باستخدام خطوط (PRI) للمركز الرئيسي واستخدام خطوط الاتصال (UP DIAL) للمستخدمين بخواص (ISDN) لسرعات تصل ما بين ٦٤ كيلو بايت إلى ١٢٨ كيلو بايت، كما استخدمت الخطوط المؤجرة (LEASE LINE) في بعض القطاعات والمديريات للدخول إلى المركز الرئيسي، وتصل الطاقة الاستيعابية لعدد المستخدمين لشبكة الإنترنت إلى ٥٠٠ مستخدم لحظياً، أما الآن يتم الاعتماد على الشبكة الاستراتيجية لوزارة الداخلية بالإضافة إلى شبكة (الواي ماكس).

٢- الحاسبات الآلية (Web Server) :

يتم استخدام الحاسبات الآلية كما يلي :

أ- حاسبات الويب الرئيسية (MAIN WEB SERVER) :

تحتوي حاسبات الويب على البوابة الرئيسية لشبكة معلومات وزارة الداخلية (MAIN PORTAL)، ويمكن من خلال البوابة الرئيسية الدخول إلى كافة مواقع جهات الوزارة سواء المحملة على الحاسبات الخادمة بالمركز الرئيسي أو المحملة على الحاسبات الخادمة بجهات الوزارة.

ب- حاسبات قواعد البيانات (DATABASE SERVER) :

تتمتع حاسبات قواعد البيانات بإمكانية تخزين عالية مع استخدام تكنولوجيا (CLUSTER) في تخزين وتداول البيانات.

ج- حاسبات تأمين الاتصالات (REMOTE ACCESS SERVER) :

شبكة الإنترنت هي شبكة معلومات مغلقة وغير مصرح لأي جهة غير أمنية الدخول إلى مواقعها، وقد تم استخدام حاسبات تأمين الدخول تعمل على قنوات اتصال (PRI) لاختيار رقم طالب الخدمة، ويصرح فقط للأرقام المسموح لها بالدخول لتصفح مواقع الشبكة.

د- حواجز التأمين (FIRE WALL) :

رعى فى إنشاء شبكة المعلومات اتخاذ كافة التدابير الأمنية فى تداول ونقل البيانات باستخدام تكنولوجيا التشفير وحاسبات الحائط النارى (FIRE WALL) كما استخدم نظم التأمين (ISA FIRE WALL) لتأمين الدخول على التطبيقات بالشبكة.

٣- نظم إدارة شبكات الاتصال :

تم دعم شبكة المعلومات بنظم تشغيل الإدارة الشبكات عن بُعد للوقوف على مشاكل التشغيل سواء لخطوط أو أجهزة الاتصال أو الحاسبات الخادمة والحاسبات العميلة، مع توافر إمكانية التداخل عن بُعد لمعالجة كافة مشاكل الشبكة.

مقومات شبكة الإنترنت :

تعدد خدمات البوابة الرئيسية لشبكة معلومات وزارة على الإنترنت، وقد تم تصنيفها إلى ثلاثة محاور رئيسية هي:

■ المحور الأول - إعلامى :

يهدف إلى إعلام الضباط والعاملين بالوزارة بتوجيهات القيادات العليا والقرارات الوزارية والكتب الدورية وأهم الأحداث الأمنية الجارية، وأوجه الرعاية الاجتماعية والصحية التى تقدمها الوزارة.

● المحور الثانى - الاستعلام :

يهدف المحور الثانى إلى إجراء الاستعلامات المطلوبة من خلال التطبيقات الأمنية بالشبكة، ويمكن من خلال الشبكة فحص المشتبه فيهم من خلال قاعدة بيانات مصلحة الأمن العام، والاستعلام عن السوابق والالتزامات أو بيانات المحكوم عليهم الهاربين، كما تتيح تطبيقات الغياب والمفقودين من التعرف على الجثث المجهولة، وكذا

الاستعلام عن السيارات التي يتم ضبطها والتعرف على السيارات المبلغ بسرقتها، كما يمكن الاستعلام عن الكتب النورية والقرارات الوزارية والقوانين التي تخدم معظم مجالات العمل وغير ذلك من الخدمات الصحية والاجتماعية التي تقدمها الوزارة.

• المحور الثالث - تبادل البيانات :

تم توفير خدمة البريد الإلكتروني عبر شبكة الإنترنت، وقد تم تنفيذ تطبيق البريد الإلكتروني اعتماداً على الكوادر الفنية المتخصصة من ضباط الوزارة لتحقيق خصوصية الاستخدام وسهولة التعامل مع أدوات التطبيق باللغة العربية لتبادل رسائل بين كافة جهات الوزارة في إطار من السرية والسرعة وتداول المكاتبات بهدف تحقيق شعار «حكومة بلا أوراق».

رابعاً - أهداف تكنولوجيا المعلومات الأمنية :

استخدام تكنولوجيا المعلومات الأمنية في مجالات الحياة المعاصرة أصبحت علامة مميزة وضرورة عصرية لا غنى عنها، وهدف استراتيجي في إطار السياسة الأمنية المعاصرة، بغية تدعيم القيم الإنسانية والأخلاقية، واحترام القانون وسيادة الشرعية الدستورية، وصيانة حقوق الإنسان، وترسيخ قواعد العدالة الجنائية، والارتقاء بمستوى الخدمات الأمنية الجماهيرية، وباعتبارها النبض والعصب لجهود التنمية الاقتصادية والاجتماعية، والثقافية، والعلمية.

وانطلاقاً من هذا المفهوم، قامت وزارة الداخلية المصرية بتنفيذ عدداً من المشروعات المعلوماتية، بدءاً من مشروعات الميكنة والتطوير التي كان متعارف عليها من قبل، ووصولاً إلى مشروعات التنمية المعلوماتية والحكومة الإلكترونية، التي تمثل قمة التحديث الحالي، بغية تحقيق الأهداف الآتية :

- مواكبة التطور السريع والمذهل في تكنولوجيا الحاسبات الآلية، من خلال

الفصل الثاني - تكنولوجيا المعلومات الأمنية

التطوير المستمر لآليات العمل الأمني، بما يضمن الارتقاء بمستوى أداء الأجهزة الشرطية.

- الارتقاء بمستوى الأداء للعاملين، من خلال وجود الأدوات المعلوماتية والأنظمة الاتصالية، مما يخلق لديهم الحوافز الشخصية للابتكارات والمهارات، ويختصر الوقت والجهد ويحسن الأداء.

- سرعة الاستجابة للمواقف الأمنية، بتوفير المعلومات والبيانات القادرة على التعامل مع متغيرات الأحداث على الأصعدة القومية والإقليمية والدولية.

- دعم مقومات الأمن والاستقرار اللازم لمسيرة العمل الوطني، وتشجيع الاستثمار الوطني والأجنبي، وتحقيق التنمية الشاملة، من خلال توفير البيانات الحديثة والمعلومات الدقيقة اللازمة لتأمين متطلبات المجتمع.

- العلاقة بين الشرطة والشعب وتوثيق أوجه التعاون بينهما، باستخدام التقنيات المعلوماتية المتقدمة وتقديم خدمات أمنية أفضل وأيسر للمواطنين، والعمل على تبسيط وتيسير إجراءات حصولهم على الخدمات الشرطية.

خامساً - خصائص ومميزاتها المعلومات الأمنية :

للمعلومات أهمية في حياتنا الحاضرة فيتم الاعتماد عليها في جميع المجالات المختلفة، ويقدر توفر المعلومات المناسبة وفي الوقت المناسب، يكون دقة القرار وصحته، وتعد المعلومات مصدراً أساسياً لصنع القرارات في مجالات الصناعة والتنمية والشئون الاقتصادية والإدارية والعسكرية والسياسية والأمنية^(١).

في المجال الأمني لا بد من توافر معلومات على مستوى عالٍ من الدقة والوضوح

(١) حسن علي الزغبى : نظم المعلومات الاستراتيجية، عمان، دار وائل للنشر والتوزيع، الطبعة الأولى، ٢٠٠٥م، ص ٥١.

والسرعة لاتخاذ القرارات الأمنية في المشاكل اليومية المتجددة، ولوضع الاستراتيجيات والخطط الأمنية للفترة القادمة لمواجهة أى خروج على الشرعية محتمل الحدوث، وحتى تصبح المعلومات الأمنية ذات فائدة للعرض على متخذي القرار يراعى فيها توافر بعض الخصائص، ومن أهمها ما يلي:

١- النطاق الزمني، فقد تكون المعلومات تاريخية أو مستقبلية، وتستخدم المعلومات التاريخية لمراقبة ومراقبة الأداء أو تصميم حلول بديلة لمشاكل روتينية، أما المعلومات المستقبلية تستخدم للتنبؤ بحلول لمشاكل مستقبلية ومعايير رقابية لها.

٢- الشكل الذى تقدم فيه المعلومات، فقد تكون ملخصة أو تفصيلية، فالمعلومات الملخصة تعتبر كافية للتعرف على المشكلة، أما المعلومات التفصيلية تستخدم لاتخاذ القرارات في المستويات القيادية ومراحل اتخاذ القرار.

٣- المعلومات قد تكون متوقعة أو غير متوقعة، والمعلومات المتوقعة تزيد فيها نسبة التأكد طبقاً لدرجة التوقع، والدور الأساسى لنظم المعلومات هو تقديم معلومات غير متوقعة وهى تستخدم لاكتشاف المشاكل من خلال الإنذار المبكر.

٤- مصادر المعلومات، فهناك مصادر داخلية وخارجية. المصادر الداخلية مثل معدلات تنفيذ الأحكام خلال فترة، معدلات ارتكاب جرائم معينة خلال فترة، معدلات ضبط القضايا، أما المصادر الخارجية تمثل بيانات عن المنشآت المهمة في منطقة ما، أو الشخصيات المهمة في دائرة معينة، ويجب توافر النوعين من البيانات ولا يكفى الاعتماد على نوع واحد^(١).

(١) محمد العمود خضبة : نظم المعلومات للأمن والتكنولوجيا، دار الإشعاع للطباعة، القاهرة، ١٩٨٧م، ص ٥٥.

الفصل الثاني - تكنولوجيا المعلومات النهائية

٥- درجة تنظيم المعلومات، هناك معلومات منظمة ومعلومات غير منظمة، المعلومات المنظمة تعكس كافة المعلومات التي تحتويها بصورة واضحة وبقية، أما المعلومات غير المنظمة فهي تقدم بشكل لا يفصح عما تحتويه من معلومات ولا تساعد متخذ القرار للاستفادة منها.

٦- درجة الدقة في المعلومات، وتتحدد بما تمثله المعلومات للموقف أو الحدث الذي تصفه وطبيعة المشكلة والعوامل التي تؤثر عليها، وقدرتها على توفير اتجاه معين لدى متخذ القرار.

٧- درجة الرسمية للمعلومات، المعلومات قد تكون رسمية وهي المعلومات التي تخرجها الجهة أو جهات أخرى معتمدة محددة المصدر كالتقارير أو الإحصائيات أو الخطابات الرسمية وتقدمها نظم المعلومات، أما المعلومات غير الرسمية فهي التي تأتي للنظام عن طريق غير رسمي وغير مصدر المصدر، أو معتمد من جهة أخرى.

٨- درجة التغير، فالمعلومات قد تكون ثابتة أي غير قابلة للتغيير، ومعلومات قابلة للتغيير، مثال لذلك أسماء الضباط وتاريخ الميلاد ورقم الأقدمية هي معلومات غير قابلة للتغيير وعند حدوث تغيير فيها يشكل خطأ يجب مراجعته، أما الحالة الاجتماعية ومحل الإقامة ومكان العمل فهذه المعلومات قابلة للتغيير.

٩- خاصية المرونة، فالمعلومات ذات قدرة على إعادة التشكيل وإعادة الصياغة، فعلى سبيل المثال يمكن تمثيل المعلومات في صورة قوائم أو أشكال بيانية أو رسوم متحركة أو أصوات ناطقة.

١٠- قابلية نقلها عبر مسارات محددة لفئة معينة، أو بثها على المشاع لمن يرغب في استقبالها من خلال شبكات الحاسبات أو وسائل نقل المعلومات المختلفة.

١١- قابلية الاندماج العالية للعناصر المعلوماتية، فيمكن بسهولة تامة ضم عدة قوائم في قائمة أو تكوين نص جديد من فقرات يتم استخلاصها من نصوص سابقة^(١).

١٢- خلافاً للموارد المادية التي تنتهي مع الاستهلاك، لا تتأثر موارد المعلومات بالاستهلاك، بل على العكس، فهي - عادةً ما - تقو مع زيادة استهلاكها لهذا السبب فهناك ارتباط وثيق بين معدل استهلاك المجتمعات للمعلومات وقدرتها على توليد المعارف الجديدة.

١٣- سهولة النسخ؛ حيث يستطيع مستقبل المعلومة نسخ ما يتلقاه من معلومات بوسائل يسيرة للغاية وبشكل ذلك عقبة كبيرة أمام تشريعات الملكية الفكرية الخاصة للمعلومات^(٢).

١٤- إمكان استنتاج معلومات صحيحة من معلومات غير صحيحة أو مشوشة، وذلك من خلال تتبع مسارات عدم الاتساق والتعويض عن نقص المعلومات غير المكتملة وتخليصها من الضوضاء.

سادساً - معايير جودة المعلومات الأمنية :

يقصد بجودة المعلومات الأمنية قدرتها على تحقيق القائد متخذ القرار لاستخدامها ليهتخذ موقفاً معيناً أو صدور قرار ما، يتناسب مع ما وفرته هذه المعلومات من اتجاهات معينة لدى متخذ القرار، وجودة المعلومات لا تتحدد بدرجة الدقة والمصدقية الموجودة في المعلومة، ولكن اعتماداً على وجهة نظر متخذ القرار ومدى رضاه عن تلك المعلومات. ولتحديد درجة الرضا عن المعلومات هناك ثلاثة عوامل رئيسية يعتمد عليها، وهي:

(1) Bhunia C.T, : Information Technology Network, New AGE, 2005, p45.

(2) O'Brien, James A : Management Information Systems, Third Ed, Chicago: Irwin, 1996, p92.

١ - منفعة المعلومات:

المعلومات يتم تقييمها من زاوية المنافع الأمنية التي تتحقق نتيجة استخدام هذه المعلومات أو نتيجة دورها في تحفيز الضابط متخذ القرار على استخدامها، ويمكن تحديد المنفعة الأمنية المرتبطة بسهولة الاستخدام وتتضمن أنواع المنافع الآتية^(١):

- المنفعة الشكلية:

يُقصد بها اقتراب شكل المعلومة التي تقدم للضابط لتتخذ القرار مع متطلباته وبصورة تجعلها قابلة للاستخدام الفوري^(٢).

- المنفعة الزمنية:

تُقاس تلك المنفعة بتوقيعات توافرها منذ لحظة الاحتياج لها وتتنزايد المنفعة الزمنية كلما أتمت المعلومات في توقيعات تسمح بتحليلها واستخدامها في اتخاذ القرارات الأمنية، والمعلومات التي تتوافر بعد اتخاذ القرار الأمني، قد يكون لها منفعة في تصويب القرارات أو تقليل الآثار السلبية الناتجة عنها^(٣).

- المنفعة المكانية:

يُقصد بها سهولة الوصول إلى المعلومة، ففي بعض الأحيان تكون المعلومات متوافرة في الجهة ويصعب الوصول إليها وقت الحاجة لسوء الحفظ أو لقصور في التطبيق لاستخراج تقارير وإحصائيات معينة في حاجة إليها.

- منفعة التملك:

يُقصد بها إدارة المعلومات والتحكم فيها وهي تمثل تملك إحدى الإدارات الفرعية

(١) إسماعيل محمد محمد السيد: نظم المعلومات لاتخاذ القرارات الإدارية، الإسكندرية، للكتب العربي الحديث للطباعة والنشر، ٢٠٠١م، ص ١٠٧.

(2) O'Brien, James A, op. cit, P127.

(٣) طارق ملة: نظم المعلومات والحاسبات الآلية من منظور إداري، القاهرة، دار الفكر العربي، ٢٠٠٨م، ص ٩٥.

للمعلومات، وعدم مشاركة تلك الإدارة في اتخاذ القرار أو عرض المعلومات مما يؤثر على تكامل المعلومة لدى الجهة ووجود قصور فيها نتيجة عدم الحصول على كافة المعلومات المتاحة لدى الجهة.

وتتمثل منفعة المعلومات في القيمة التي يتم إضافتها للمستخدم من خلال تلك المعلومات، وبالتالي تؤدي إلى المساعدة في اتخاذ القرارات^(١).

٢- درجة الرضا عن المعلومات من قبل القائد متخذ القرار:

تعد درجة الرضا شيئاً نسبياً للقائد متخذ القرار، فمن الصعب أن نحكم على القدر الذى ساهمت به المعلومات في عملية اتخاذ القرار، ولكن البديل الذى يمكن عمله هو استخدام مقياس لمدى رضا متخذ القرار عن المعلومات المقدمة إليه، ويرجع ذلك إلى مدى توافر المعلومات المطلوبة لدى متخذ القرار وضمن توفير تلك المعلومات، هل ساهمت المعلومات في توفير معرفة عن المشكلة أو الأزمة لدى متخذ القرار أم أن هناك تأخيراً في استخراج تلك المعلومات؟ فيتم اتخاذ القرار بدون الاعتماد على تلك المعلومات وهل أسلوب العرض كان مناسباً وسهلاً؟ وهل كانت المعلومات واضحة ومباشرة؟ كل تلك العناصر تؤثر على مدى رضا القائد متخذ القرار^(٢).

٣- درجات الخطأ والتحيز في المعلومات:

في اتخاذ القرارات تفضل القيادات جودة المعلومات على كمية المعلومات، وجودة المعلومات تتفاوت باختلاف درجة الخطأ والتحيز، والمشكلة تكمن في أن مستخدم المعلومات لا يكون على علم بدرجة الخطأ أو التحيز، ولا يمكنه إدراك أن هناك خطأ أو تحيز في البيانات، وإلا كان من السهل تعديل تلك المعلومات للقضاء على التحيز.

(١) أشرف السعيد أحمد: تكنولوجيا المعلومات وإدارة الأزمات، القاهرة ٢٠١٢م، ص ٦٧.

(2) O'Brien, James A, op. cit, p116.

الفصل الثالث - تكنولوجيا المعلومات الأمنية

والأخطاء تمثل - أيضًا - مشكلة سواء كانت بدون قصد أو متعمدة.

ويرجع وجود خطأ في المعلومات لعدة أسباب من أهمها:

- استخدام طريقة غير دقيقة في جمع البيانات.
- إتباع طريقة غير سليمة في إعداد البيانات في صورة معلومات.
- فقد جزء من البيانات أو ترك بعضهما بدون تشغيل.
- الخطأ غير المقصود في إدخال البيانات.
- استخدام ملف خاطئ في حفظ البيانات.
- الخطأ في البرامج المستخدمة لإعداد البيانات باستخدام الحاسب الآلي.
- التزوير المتعمد في البيانات.

هناك عدة طرق تقلل من نسبة الخطأ في المعلومات المتاحة ومنها ما يلي:

- وجود نظام مراجعة على عملية إدخال المعلومات.
- وجود نظام رقابة داخلية على المعلومات لاكتشاف الأخطاء.
- وضع قواعد خاصة بعمليات الإعداد والتجميع للبيانات^(١).

العمر الزمني للمعلومات:

يُقصد بالعمر الزمني للمعلومات تلك الخاصية الزمنية المتعلقة بالمعلومات التي يتم تحويلها إلى تقارير وإحصائيات، ويوجد نوعان من تلك البيانات وهي:

- البيانات في تاريخ محدد:

يُقصد بها البيانات التي تتعلق بنقطة زمنية محددة بتاريخ معين مثال لذلك عدد قضايا المخدرات التي تم ضبطها حتى ٢١/١٢/٢٠١٢م.

(١) أشرف السعيد أحمد: أثر تكنولوجيا الأزمات على إدارة الأزمات الأمنية (دراسة تطبيقية)، القاهرة، ٢٠١١م، ص ٧٧.

- البيانات عن فترة محددة:

يُقصد بها البيانات التي تعبر عن أي تغير خلال فترة زمنية معينة، مثال لذلك عدد قضايا المخدرات التي تم ضبطها خلال شهر مارس ٢٠١٢م.

ولتوضيح مفهوم العمر الزمني للمعلومات وقياسه ينبغي أن نتعرض لمصطلحين أساسيين وهما:

فاصل المعلومات الزمني:

يُقصد به المسافة الزمنية بين تقريرين متتاليين من النوع نفسه، فالتقارير الأسبوعية الفاصل الزمني لها أسبوع، والتقارير الشهرية الفاصل الزمني لها شهر، ويرمز إلى الفاصل الزمني بالرمز (س) ^(١).

التأخير في إصدار المعلومات:

يُقصد به التأخير الزمني الذي يستغرق في إعداد المعلومات للنشر في صورة تقرير ويقاس بالفترة الزمنية بين نهاية الفاصل الزمني للمعلومات وصدور التقرير الجديد للاستخدام، ويرمز للتأخير في إعداد المعلومات بالرمز (ص).

وباستخدام هذين المصطلحين (فاصل المعلومات الزمني «س»، التأخير في إعداد المعلومات «ص») يمكن حساب الحد العمري الأقصى، والحد العمري المتوسط، والحد العمري الأدنى للمعلومات، ويعبر الجدول التالي عن تلك العلاقة:

نوع الحد العمري للمعلومات	التأخير في إعداد المعلومات
الحد العمري الأقصى	ص + س
الحد العمري المتوسط	ص + ٠,٥ س
الحد العمري الأدنى	ص

جدول (١-٢) الحد الأقصى والمتوسط والأدنى لعمر المعلومات

(1) Collin, S. M. H : Dictionary of Technology, London: Peter Collin Pub, 1996, p141.

يمثل الجدول السابق أسلوب قياس الحد العمري للمعلومات في تاريخ معين ومثال لذلك الحد العمري الأدنى للمعلومات، وتمثل في زمن التأخير في إعداد المعلومات، لو كنا بصدد إعداد تقرير عن معدلات تنفيذ الأحكام عن شهر مارس ٢٠١٢م، ومعدل التأخير في إعداد التأخير هو خمسة أيام وهو وقت تجميع البيانات وإعداد التقرير المطلوب، فإن الحد العمري الأدنى لصدور التقرير هو ٥/٤/٢٠١٢م، وهو التاريخ المحدد لصدور التقرير فإن زاد على ذلك يكون هناك تأخير في صدور التقرير، والعمر الأقصى هو معدل التأخير في إعداد المعلومات ويضاف إليه فاصل المعلومات الزمني، بمعنى أن هذا التقرير يعد صالحاً للاستخدام حتى تاريخ ٥/٥/٢٠١٢م، وهو تاريخ صدور التقرير التالي عن شهر أبريل.

والعمر الزمني للمعلومات يمكن التأثير عليه من خلال التقرير في معدل التأخير في إعداد المعلومات بإتباع أساليب التخزين الحديثة والإدخال المباشر للبيانات واستخراج التقارير مباشرة فعندما نصل إلى درجة تأخير تساوى صفر فإن الحد العمري للمعلومات سواء الحد الأدنى أو الأقصى تصبح تساوى الفاصل المعلومات الزمني^(١).

سابقاً - تكنولوجيا المعلومات وصنع القرار الأمني :

جوهر العمل في مجال الشرطة هو صنع القرارات، فالعمل الشرطي يحتاج إلى اتخاذ قرارات يومية عديدة في مواقف مختلفة، والقائد الناجح يتوقف نجاحه على مدى قدرته على صنع القرار، وهو اختيار بين عدة بدائل استجابة لموقف معين، كتحديد قوة أمنية لكمين شرطي، أو تحديد موقع معسكر قوات أمن واختيار بين عدة بدائل مختلفة لكل منها مميزات وعيوب مختلفة، ويتوقف نجاح القيادة على مدى فاعليتها في اتخاذ قرارات فعالة ورشيده، لإحداث التغيير داخل المنظمة في أدائها لوظائفها،

(1) Collin, S. M. H, op. cit, p143.

والفاعلية ليست قدرة فطرية ولكن يمكن اكتسابها وتنميتها، ولذا يتم إلقاء الضوء على طبيعة عملية اتخاذ القرارات ومراحل صنع القرارات.

دور نظم وتكنولوجيا المعلومات في صنع القرار الشرطي :

تعمل تكنولوجيا المعلومات في الجهات الشرطية على تخفيض عدد قنوات الاتصال، بين القائد ومرؤوسيه (الاتصالات الهابطة)، وبين المرؤوسين والقائد (الاتصالات الصاعدة)، أو بين المستوى الإداري الواحد (الاتصالات الأفقية)؛ مع القدرة على انتشار أوسع في المشاركة بالمعلومات ما بين المستويات الإدارية المختلفة في ظل تباعد المسافات، والاستعانة بالأشخاص الذين يمتلكون الخبرة لإضافة المعلومات التي يحتاجها صانع القرار، فلا يوجد في المنظمة مستويات إدارية متعارضة، ولكنها تكون متكاملة ويؤدي تطبيق تكنولوجيا المعلومات لتطوير نظم المعلومات الأمنية المستخدمة، وتوزيع المهام بدقة وتدفق المعلومات المطلوبة إلى صانعي القرار الأمن في الوقت المناسب.

وهناك عدة مهام نعمل من أجلها، وهي :

- ١- سهولة العمل الذي يهدف إلى دعم جميع المشاركين في العمل الشرطي بإمدادهم بمخرجات ذات جودة عالية وفاعلية كبيرة.
- ٢- زيادة قدرة رجال الشرطة على حل المشاكل وبناء العلاقات وحسن الود مع الجمهور.
- ٣- زيادة تحقيق أنشطة منع الجرائم والقدرة على عمل التحريات وأعمال البحث الجنائي وتحقيق نتائج إيجابية في تقليل أعمال الإخلال بالأمن العام.
- ٤- تحقق كم أكبر من المعرفة لرجال الشرطة مما يساعد على التعرف على مسببات الجرائم والعمل على منعها والقضاء عليها.

٥- استخدام أجهزة وشبكات الاتصال الحديثة المعتمدة على الحاسب الآلى تؤدي إلى سرعة استجابة قوات الشرطة للحادث وأيضاً سرعة رد الفعل عند التعامل مع الحادث.

٦- باستخدام تكنولوجيا المعلومات فإن قاعدة المعرفة ستكون متاحة لجميع العاملين في المجال الشرطى (حسب قواعد الأمن المتبعة وهى المعرفة على قدر الحاجة) وذلك يحقق عدم مركزية امتلاك البيانات والمعلومات مما يؤدي إلى سهولة اتخاذ القرارات.

٧- يتم الاستعانة بنظم المعلومات الجغرافية للاستفادة من ربط قاعدة البيانات العادية بالبيانات الجغرافية للمساعدة في اتخاذ القرار.

يتضح مما سبق أهمية الدور الذى تلعبه المعلومات فى عملية صنع القرارات، وأهمية أن تتوافر هذه المعلومات فى التوقيت والشكل المناسبين، فضلاً عن دقتها وارتباطها الوثيق بموضوع القرار الذى يصدر من جانب رجل الإدارة.

أسباب الفشل فى عملية صناعة القرار الشرطى:

يتوقف نجاح القائد فى عمله على نوعية القرارات التى يتخذها، فقد تؤدي القرارات غير الرشيدة إلى أن يكتشف بعد فترة أنه لا يقوم بأعمال كان يجب القيام بها، أو أنه غير قادر على القيام بأعمال يجب القيام بها الأمر الذى يخلق شعوراً بالإحباط والاستياء نتيجة فشله فى عمله^(١).

(1) Owen, Jo : The Leadership Skills Handbook, London; Philadelphia: Kogan Page, 2006, p59.

ويرجع السبب في فشل القرار الشرطي - غالباً - إلى ما يلي:

١ - الفشل في إعطاء الأوزان المناسبة للأولويات:

قد يرجع السبب في عدم سلامة القرارات المتخذة إلى عدم قدرة المدير على تحديد الأولويات المتعلقة بموضوع المشكلة والإخفاق في تحديد أهمية العوامل المختلفة والأوزان المقررة لكل منها^(١).

٢ - تأجيل اتخاذ القرارات بلا مبرر:

بعض القيادات لا تقوم باتخاذ القرار في الوقت المناسب، فعندما يقول المدير سوف أفكر في الأمر فيما بعد، أو أنا مشغول جداً الآن، في كل تلك الأحوال يكون هناك اتخاذ قرار، وهو تأجيل اتخاذ القرار، ولا يدرك أنه يتخذ قراراً فعلياً^(٢).

٣ - الاهتمام المتزايد بالتفاصيل:

وذلك حينما يهتم المديرون بتفاصيل الموضوعات، وتقول فتاعة لديهم بأنهم مطالبون باتخاذ كل القرارات بأنفسهم ولا يعطون حرية للمستويات الأقل في اتخاذ القرارات الخاصة بهم.

٤ - تهدئة الموقف العرج:

بعض القيادات تبنى قراراتهم على الظروف المحيطة بهم، فلو أدت إحدى المشكلات إلى احتدام الموقف، فإن المدير يتخذ القرار الذي يؤدي إلى تهدئة الموقف، وإرضاء الأطراف المتضمنة، وقد يترتب على ذلك تراكم المشكلة الأصلية نتيجة لعدم اهتمامه بها وبحلها، واهتمامه بالأمور العرضية التي تسبب إزعاجاً لسير العمل، وغالباً ما ينتج

(١) عبد الحكم أحمد الخراسي، فن اتخاذ القرار داخل تطبيق، مكتبة ابن سينا للنشر والتوزيع، القاهرة ١٩٩٦م، ص ٥٢.

(2) Owen, Jo, op.cit, p65.

من هذه القرارات الوقتية سلسلة من المشكلات تظهر فيما بعد^(١).

٥ - الإفراط في استخدام معيار الصواب والخطأ

بعض القيادات يحاولون الوصول إلى تحليلات كاملة للموقف، ولا تكون هذه المجموعة على استعداد لاتخاذ القرار إلا عندما تتضح أمامها الرؤية الكاملة لكل متغيرات ومحددات الموقف، ولهذا فإنها تشعر بصعوبة بالغة في تحديد الصواب والخطأ، وقد يؤدي هذا الاتجاه إلى عدم الوصول إلى قرارات إدارية سليمة، نظرًا لأن متغيرات الموقف الإدارية المختلفة لا تتضمن بالضرورة جوانب صحيحة مطلقة أو جوانب سلبية مطلقة.

٦ - التفاؤل المبني على التخمين

بعض القيادات يثقون بخبراتهم في اتخاذ القرارات الصائبة بدرجة كبيرة، وقدراتهم على الإحساس بالنتائج عن طريق التخمين وليس الدراسة، وهم -غالبًا- أصحاب نجاحات كثيرة في مجال اتخاذ القرارات، ربما لأنهم كانوا يعتمدون في بداية حياتهم العملية على البيانات الواقعية في اتخاذهم للقرارات، أو نجاح ولید الصدفة والظروف، وعندما تقدموا في مجالهم الوظيفي وشغلوا مناصب قيادية وزادت مشاغلهم، اعتمدوا على النجاحات السابقة، والقدرة على التخمين والتوقع ولم يقوموا بالجهود السابقة نفسها في البحث عن الحقائق اللازمة لاتخاذ القرارات^(٢).

٧ - النظرة الضيقة للأمور

إن المنظمة نظام متكامل، ومهما كان القرار الذي يتخذ ويبدو أنه متعلق بأمور مستقلة، كان يخص قسمًا أو إدارة ما أو نشاط معين فهو في النهاية يؤثر ويتأثر بباقي الأقسام والإدارات والأنشطة، وبعض القيادات تكون نظرتهم للأمور ضيقة ويعتبرون أنفسهم بمعزل

(1) Fletcher, Keith, op.cit, P117.

(2) Fletcher, Keith, op.cit, P118.

عن بقية أجزاء المنظمة، ويمجزون عن إدراك كل الجوانب اللازمة لاتخاذ القرار، وغالباً ما يواجهون بمشاكل فيما بعد عندما يتطلب الأمر منهم مواجهة المتغيرات العديدة التي يتطلبها اتخاذ القرار.

معوقات اتخاذ القرار الشرطي:

تتعدد وتتوغل المشاكل التي تواجه اتخاذ القرار الشرطي، وهذه المعوقات والمشاكل إما إدارية أو بيئية أو ترجع إلى طبيعة العمل الشرطي ومن أهم تلك الأسباب⁽¹⁾:

١- المركزية في سلطة اتخاذ القرارات وعدم تفويض السلطة لاتخاذ القرارات دون الرجوع للقيادات الأعلى.

٢- عدم وضوح الأهداف الأمنية والخطط وسريتها لدى بعض القيادات الشرطية قد يجعل الرؤية غير واضحة ومكتملة أمام صانع القرار في عمليات التنبؤ.

٣- عدم إحساس بعض القيادات بالاطمئنان والأمان عند اتخاذهم القرارات خوفاً من المسؤولية لكثرة اللوائح والقرارات والأوامر الدورية، والخوف من عدم الإلمام بها يؤدي إلى الإحجام عن اتخاذ القرار والرجوع إلى رؤسائهم في كل كبيرة وصغيرة لأخذ الموافقة على اتخاذ القرار للاطمئنان إلى صحة وسلامة القرارات وانسجامها مع سياسية الوزارة والقيادات.

٤- تشابك العلاقات والمصالح في المشكلة أو الموقف الذي يواجهه ضابط الشرطة ويصعب التعرف على الأبعاد المختلفة.

٥- بعض القيادات يبنون قراراتهم على الظروف المحيطة بهم، بمعنى أنه لو أدت إحدى الأزمات إلى احتدام الموقف، فإن القائد يتخذ القرار الذي يؤدي إلى

(1) Rosenthal, Uriel, Pijnenburg, Bert : Crisis Management and Decision Making, Dordrecht ; Boston :Kluwer Academic Publishers, 1991, P93.

تهدئة الموقف وإرضاء الأطراف المتدمرة، ويترتب على ذلك تراكم المشكلات الأصلية نتيجة لعدم الاهتمام بها وبحلولها والاهتمام المطلق بالأمور العرضية التي تسبب إزعاجاً لسير العمل، وغالباً ما ينتج عن هذه القرارات الوقتية سلسلة من المشكلات والأزمات^(١).

٦- عدم وجود معيار ثابت يمكن به قياس رشد القرار؛ حيث إن رشد القرار يختلف من شخص إلى آخر ولو تم اتخاذ القرار في الظروف نفسها وذلك لنسبية عملية تقييم نتائج القرار وهل حقق القرار أهدافه كاملة أم ناقصة ؟

٧- التأخير في اتخاذ القرارات بلا مبرر لدى بعض القيادات وتأجيل اتخاذ القرار ظناً منهم انتهاء الأزمة، وأنها سوف تحل دون التدخل.

٨- بعض القيادات يثقون بدرجة كبيرة بخبراتهم وقدراتهم على الإحساس وتوقع النتائج عن طريق التخمين والشعور الداخلي.

٩- تنوع وتباين الجهات التي تحدث بها أزمات، وتعدد تلك الجهات تحتاج إلى تنسيق في اتخاذ القرار والمواجهة ودراسات عديدة، في ظل عدم وفرة المعلومات المتكاملة اللازمة لاتخاذ القرار.

ثامناً - مدى الحاجة لتكنولوجيا المعلومات في العمل الأمني :

تظهر أهمية تكنولوجيا المعلومات ومدى الحاجة إليها في المجالات الأمنية المختلفة وبصفة خاصة في مجال إدارة الأزمات الأمنية، وطبيعة العمل الشرطية هناك أزمات أمنية مختلفة وبصفة الدوام وقد تكون يومية، وهناك الحاجة إلى معلومات سريعة ودقيقة وصحيحة ومحدثة وعرضها بأسلوب مناسب، فطبيعة إدارة الأزمات تعتمد

(١) أشرف السعيد أحمد: أثر تكنولوجيا المعلومات على إدارة الأزمة الأمنية، مرجع سابق، ص ١٢٦ وما بعدها.

على اتخاذ قرار سريع، والقرار يعتمد على المعلومات المتاحة، فكلما توافرت معلومات بصورة سريعة كان القرار سريعاً، وكلما كانت المعلومات دقيقة وصحيحة كان القرار صائباً ومن أهم أسباب الحاجة لتكنولوجيا المعلومات ما يأتي:

١ - الحاجة إلى السرعة في الحصول على المعلومات:

حتى نتمكن من عرض المعلومات المطلوبة بالسرعة المناسبة يراعى توافر نظام معلومات تتوافر فيه البيانات المختلفة للحصول على المعلومات المطلوبة في أى مجال أمنى أو يتعلق بإدارة الأزمات الأمنية وتوافر من المصدر المباشر لها.

٢ - الحاجة إلى معلومات دقيقة :

أثناء المشكلات الأمنية نلاحظ التسابق في عرض كم هائل من البيانات والمعلومات، مما قد يحدث شيئاً من عدم الدقة أو تعارض في المعلومات، مما يؤدي إلى إضاعة وقت ومجهود فريق إدارة البحث في فرز تلك المعلومات، والتحقق من صحتها، وعرض معلومات غير مطلوبة تؤدي إلى عدم التركيز، والدخول في مشاكل أخرى فرعية لا علاقة لها بالمشكلة الحالية، مما يوضح لنا مدى أهمية الحاجة إلى الدقة في المعلومات.

٣ - الحاجة إلى معلومات حديثة:

يتم جمع البيانات من جهات عديدة داخل نظام المعلومات، ونلاحظ - أحياناً - أن تلك البيانات لا يتم تحديثها إلا عند الحاجة إليها، مما يضيع الوقت في عملية التحديث، وعدم الاعتماد وفقد الثقة بنظام المعلومات الحالي؛ حيث إن المعلومات الناتجة عنه قد تكون غير صحيحة لعدم تحديث قاعدة البيانات.

٤ - الحاجة إلى أسلوب مناسب لعرض المعلومات:

يعد أسلوب عرض المعلومات من أهم العوامل المؤثرة في اتخاذ القرار؛ حيث إن

الفصل الثاني - تكنولوجيا المعلومات النونية

عرض المعلومة بأسلوب ما، قد يؤدي إلى تحول القيادات إلى اتجاه مختلف، وهنا تظهر عملية التهوين والتحويل، التي تعد من أكبر المشاكل في أسلوب عرض المعلومات؛ حيث يعتمد القائم بعرض الأزمة تهوين الموقف خوفاً من المسؤولية، أو تهويل الموقف للظهور بمظهر القائد القوي المسيطر المتحكم أمام قياداته.

الفصل الثالث

استراتيجية أمن المعلومات

الفصل الثالث استراتيجية أمن المعلومات

تقديم:

إن التطور الهائل الذي يعيشه العالم في تقنية المعلومات، يحتم على كل دولة ومجتمع مواكبة هذا التطور والعمل على اكتمال حلقات منظومة المعلوماتية بدءاً بالأنظمة ومروراً بالبنية التحتية، وانتهاءً بالكوادر الوطنية المؤهلة، وقد شملت تلك التقنية قطاعاً واسعاً من وسائل نقل وتخزين وبحث المعرفة، فكان لا بد من تأمين شبكة المعلومات من الاختراق، ووضع استراتيجية وسياسة لتأمين للمعلومات. لكل منشأة أسلوبها الخاص في توفير الأمن من المخاطر محل التحديد ويحدود متطلبات حماية المعلومات التي تم تحديدها وإمكاناتها المادية والميزانية المخصصة للحماية، فلا تكون إجراءات الأمن رخوة ضعيفة لا تكفل الحماية ولا مبالغاً بها إلى حد يؤثر على عنصر الأداء في النظام محل الحماية، معالجة أوجه القصور والمعوقات، والعمل على تطوير تقنية المعلومات.

وفي ضوء ما تقدم، سنتناول هذا الموضوع على النحو الآتي :

أولاً، مفهوم أمن المعلومات.

ثانياً، مفهوم الاستراتيجية.

ثالثاً، محل الحماية.

رابعاً، المخاطر المحتملة.

خامساً، أهم أساليب تأمين قواعد البيانات.

أولاً - مفهوم أمن المعلومات :

إن التطورات الحديثة في تقنية المعلومات أحدثت تغيرات مستمرة بأساليب العمل في كثير من المجالات وكافة نواحي الحياة المختلفة، وأصبحت عملية انتقال وتوصيل المعلومات عبر الشبكات المحلية والدولية من الأمور الروتينية في عصرنا الحالي وإحدى علامات العصر المميزة التي لا يمكن الاستغناء عنها لتأثيرها الواضح في تسهيل العديد من الخدمات ومتطلبات الحياة العصرية، وقلة كلفة استعمالاتها مما كانت عليه، في ظل عصر الثورة المعلوماتية والتقدم العلمي الكبير، ما زالت القرصنة الإلكترونية مشكلة تؤرق وتهدد الجميع لما لها من تداعيات وخيمة على سلامة المجتمع وأمنه، فهناك تطور سريع في عمليات الاختراق وتقنيات وأساليب القرصنة، وأصبحت هذه التقنية الحديثة للمعلومات سلاحاً ذو حدين تحرص المنظمات على اقتناؤه وتوفير سبل الحماية من الاختراق وتحديد الاستراتيجيات والإجراءات الدفاعية والوقائية من الاختراق أو التخريب، فكان لأمن المعلومات الأهمية الكبرى في الحفاظ على تلك التقنية من الخطر المدمر لها.

أمن المعلومات (Information Security) :

مع تزايد القيمة الاقتصادية للمعلومات وتطور العلم والتكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة عبر الشبكة من موقع لآخر زاد الاهتمام بأمن نظم المعلومات والاتصالات بشكل مهم للغاية؛ حتى أصبحت تلك النظم تمثل عاملاً رئيسياً في إدارة جميع القطاعات المختلفة، ووجب العمل على توفير الحماية التقنية لها، وتوفير وسائل تقنية متنامية كجدران النار وكلمات السر ووسائل التشفير البيولوجية والتشفير وغيرها، ويعرّف أمن المعلومات بأنه هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن الاعتداء عليها، والعمل على تحديد

الوسائل والأدوات والإجراءات اللازمة توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية أثناء التداول لمنع وصول المعلومات إلى أيدي أشخاص غير معنولين عبر الاتصالات ولضمان صحة هذه الاتصالات^(١).

وتعد النظم المعلوماتية وقواعد البيانات وشبكات الاتصال عصب العالم المعرفي والصناعي والمالي والصحي وغيرها من القطاعات، ويجب الحفاظ على العناصر الرئيسية لأمن المعلومات المتمثلة في السرية وسلامة المحتوى والاستمرارية وعدم إنكار التصرف، وفيما يلي سنتعرض لكل منها بالتفصيل المناسب.

السرية أو الموثوقية (Confidentiality) :

السرية تعنى ذلك المصطلح المستخدم لمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالإطلاع عليها أو الكشف عنها، أى التأكد من أن المعلومات لا يتم الإطلاع عليها من قبل أشخاص غير مصرح لهم بذلك طبقاً للصلاحيات الأمنية المحددة، وتحديد الصلاحيات المحددة لكل مستخدم ومناطق الاستخدام المسموح الدخول عليها، وأيضاً التوقيت المصرح له بالتواجد خلاله على الشبكة، وأيضاً حماية بيانات المستخدم من الإفشاء والإطلاع عليها دون إذن أو تفويض من مدير النظام.

على سبيل المثال، بطاقة الائتمان والمعاملات التجارية على شبكة يتطلب رقم بطاقة الائتمان على أن تنتقل من المشتري إلى التاجر ومن التاجر لإنجاز وتجهيز المعاملات على الشبكة، يحاول النظام فرض السرية عن طريق تشفير رقم البطاقة أثناء الإرسال، وذلك بالحد من الأماكن ظهور تسلسل رقم البطاقة (في قواعد البيانات، وسجل الملفات، والنسخ الاحتياطي، والإيصالات المطبوعة)، وذلك بتقييد الوصول إلى الأماكن التي يتم تخزين الرقم والبيانات بها، أما إذا كان الطرف غير المصرح به قد حصل

(١) أشرف السعيد أحمد : مقدمة في علوم الحاسب، القاهرة ١١٠-٢٠٠٢م، ص ٢٢٢.

الفصل الثالث - استراتيجية أمن المعلومات

على رقم البطاقة بأي شكل من الأشكال، وبذلك فقد تم انتهاك مبدأ السرية في حفظ وتخزين البيانات، والسرية أمر ضروري لكنها غير كافية للحفاظ على الخصوصية من الناس الذين يخترقون الأنظمة لسرقة المعلومات.

التكاملية وسلامة المحتوى (Integrity) :

في مجال أمن المعلومات سلامة المحتوى تعني الحفاظ على البيانات التي يتم تداولها من خلال الشبكة صحيحة ولم يتم تعديلها أو العبث بها بالتغيير من الأشخاص الغير مخول لهم بذلك، ولم يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع، عندما يقوم شخص بقصد أو بغير قصد انتهاك سلامة أو إضرار أو حذف ملفات البيانات المهمة وهو غير مخول له بذلك فهذا انتهاك لسلامة البيانات، وعندما يصيب فيروس كمبيوتر ويقوم بتعديل بيانات أو إتلافها فهذا انتهاك لسلامة بيانات، وعندما يكون الموظف قادراً على تعديل راتبه في قاعدة البيانات والمرتبات، وعندما يقوم مستخدم غير مصرح له بتخريب موقع على شبكة الإنترنت.

استمرارية توافر المعلومات أو الخدمة (Availability) :

التأكد من استمرار عمل نظام المعلومات والقدرة على التعامل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، أن تكون المعلومات متوفرة عند الحاجة إليها، وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو الوصول إليها، إذ لا يكفي الوجود بل يتعين ضمان الاستمرارية وتقديم الخدمة، والعمل على توافر نظم عالية السرية تهدف إلى استمرارية الحماية في جميع الأوقات، ومنع انقطاع الخدمة بسبب انقطاع التيار الكهربائي، أو تعطل الأجهزة، أو نظام الترقية والتحديث، والتأكد من أن الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات، والضوابط الأمنية.

المستخدمة لحمايته، وقنوات الاتصال المستخدمة للوصول إلى ذلك يجب أن يعمل بشكل صحيح^(١).

عدم إنكار التصرف المرتبط بالمعلومات (Non-Repudiation) :

ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفاً ما قد تم من شخص ما في وقت معين، والقدرة على إثبات شخصية الطرف الآخر على الشبكة وإثبات شخصية المستخدم.

وأبسط أنواع الحماية هو استخدام نظام التعريف بشخص المستخدم ومشروعيته وهذه الوسائل تهدف إلى ضمان استخدام النظام أو الشبكة من الشخص المخول بالاستخدام وتضم هذه الطائفة كلمات السر بأنواعها، والبطاقات الذكية المستخدمة للتعريف، ووسائل التعريف البيولوجية والتي تعتمد على سمات معينة في الشخص المستخدم متصلة ببيئته البيولوجي المفاتيح المشفرة ويمكن أن نضم إلى هذه الطائفة ما يعرف بالأطفال الإلكترونية التي تحدد مناطق النفاذ.

ثانياً - مفهوم الاستراتيجية :

مصطلح الاستراتيجية يعد من المصطلحات القديمة المأخوذ من الكلمة الإغريقية (Strato) وهي تعنى الجيش أو الحشود العسكرية، ومن تلك الكلمة اشتقت اليونانية القديمة مصطلح (Strategos) وتعنى فن إدارة وقيادة الحروب، وظهرت الاستراتيجية في اللغة الإنجليزية (Strategy) بقصد التخطيط للعمليات العسكرية قبل نشوب الحروب، وفي الوقت نفسه فن إدارة تلك العمليات عقب نشوب الحروب.

وبالرغم من أن أصل الكلمة (Strategy) يعود إلى التعبير العسكري، إلا أنها تستخدم

(١) أشرف السعيد أحمد : القرصنة الإلكترونية، القاهرة، ٢٠١٢م، ص ٩٠.

الفصل الثالث - استراتيجية أمن المعلومات

الآن بكثر في سياقات مختلفة مثل استراتيجيات العمل، استراتيجيات التسويق، وتعكس الاستراتيجية الخطط أو الطرق أو الأساليب المحددة مسبقاً لتحقيق هدف معين على المدى القريب أو البعيد في ضوء الإمكانيات المتاحة، واعتماداً على استخدام التخطيط والإجراءات المتوفرة التي يمكن الحصول عليها في المدى القصير.

أهداف الاستراتيجية :

تهدف الاستراتيجية إلى تحقيق هدف رئيسي تعمل من أجله سياسة المنظمة من خلال الاستخدام الأمثل لكافة الإمكانيات والوسائل المتوفرة للوصول إليه، وقد يكون الهدف سياسياً أو اقتصادياً أو عسكرياً أو معنوياً وقد يكون صغيراً محدوداً أو كبيراً. ولوصول إلى الهدف الرئيسي قد يتم وضع مجموعة من الأهداف المرحلية التي يؤدي تحقيقها إلى الهدف الاستراتيجي، وهذه الأهداف هي ما تسمى بالأهداف الاستراتيجية المرحلية، غير أن جميع الأهداف تشترك في كونها جميعاً تسعى وتعمل من أجل تحقيق الهدف الرئيسي الذي عين وحدد سلفاً من قبل السلطة السياسية العليا للمنظمة.

وسائل الاستراتيجية :

تتباين الوسائل التي تستخدمها الاستراتيجية لتحقيق هدفها تبعاً للتباين في طبيعة وأهمية ذلك الهدف وتبعاً للإمكانيات والقدرات المتاحة للظروف والأجواء المحلية والدولية السائدة، والاستراتيجية الناجحة هي التي توفق إلى اختيار الوسيلة أو الوسائل الأجدي بين كافة الوسائل المتاحة للوصول إلى هدفها، أي التي تنجح في تحقيق وتأمين التوافق بين الوسيلة والهدف وفي خلق التأثير النفسي الكافي لزعزعة ثقة الخصم بنفسه وحرمانه من حرية العمل مما سيؤدي إلى حماية المنظمة من تهديداته.

ولكى يكون اختيار الوسيلة ناجحاً فمن الضروري عمل دراسة واعية للموقف بشتى جوانبه لمعرفة العدو المطلوب قهره وتمييز نقاط ضعفه الأكثر حساسية مع تحليل عميق للتأثيرات الحاسمة التي يمكن أن تحدثها السياسة المختارة على معنويات الخصم وهذا يقتضى إنشاء مخطط استراتيجي يتضمن كافة الأعمال الممكنة وردود الأفعال المتوقعة عليها محلياً ودولياً لوضع الحلول المناسبة ليكون المخطط الاستراتيجي مترابط الأجزاء قادر على مواجهة أية مفاجآت أو ردود فعل غير ملائمة أو سيئة التأثير لضمان حرية العمل للخطة الاستراتيجية.

معايير استخدام مصطلح الاستراتيجية :

هناك معايير أساسية يجب أن تتوافر فيما يتصف بالخطة الاستراتيجية، وسنعرض لأهمها فيما يلي :

١ - مستوى التخطيط و الأهداف (الغايات) :

يقوم التخطيط بتحديد أهداف تسمى الغايات أو أهداف عليا بعيدة المدى، وهي أهداف يطلق عليها الأهداف الاستراتيجية وبناءً عليها يتم تخصيص المهام اللازمة لتحقيق هذه الأهداف، ومن ثمّ ينتقل التخطيط إلى مستوى التخطيط التبعوي والذي يحدد بدوره أهدافاً لتحقيق مهمته وتتصف بأنها أهداف متوسطة المدى أو الأهداف الفرعية والمناطق ويطلق عليها الأهداف التبعوية والتي تترجم بدورها إلى مهام تُكلف بها الوحدات الميداني، ومن ثمّ ينتقل مستوى التخطيط إلى تخطيط عالٍ المعايير يقوم بتحديد أهداف تخطيطية وهي أهداف مباشرة أو أهداف صفري، ثم تتحول تلك الأهداف إلى مهام تكلف بها كل وحدة صفري على حدة، وفي الغالب تحول هذه الأهداف إلى مستوى رابع على مستوى الفرد والقائد وهو ما يسمى الهدف المباشر، ونلاحظ أن تسلسل الخطط وتدرجها يتم من أعلى المستوى الإداري أو القيادي إلى

الفصل الثالث - استراتيجية أمن المعلومات

أسفله ، وهناك فصل بين المستويات يكون ضروري ومحسوم لما له من مميزات تفويض السلطة وتخصيص المهام وتوفير الأعباء الذهنية والتركيز في إنجاز وتحقيق المهام وتوفير قنوات الاتصال والسيطرة.

٢- وجود تهديدات أو منافسة :

يرتبط مصطلح استراتيجية بوجود وجود تهديدات ما، فالاستخدام العسكري لا يستخدم إلا في حالة وجود تهديدات تجبر المجتمعات على تكوين الجيوش، أما المنظمات غير العسكرية لا تستخدم هذا المصطلح للتخطيط لأعمالها إلا أنها تستخدم مصطلحات أخرى مثل، المنهج أو التخطيط الإداري إذا ما كان هناك هدفًا أو مجموعة أهداف تريد تحقيقها، وفي تلك الحالة لا يوجد تهديدات ومعوقات مباشرة تمنع تحقيق هذا الهدف، وتكون خطة المنظمة عبارة عن منهج ثابت ومباشر في سبيل تحقيق هذا الهدف، فالمنهج أو الخطة الإدارية ما هي إلا خطوات وخطط ثابتة في سبيل تحقيق هدف محدد، وأيضًا يمكن تقسيمه إلى مستويات تخطيطية عليا، ومستوى متوسط أو برامج أو إداري، ومستوى تنفيذي، لا حاجة لها لتكوين استراتيجية ومناورات، وفي مجال أمن المعلومات نجد أن هناك خطر أو تهديد وهو يتمثل في عملية القرصنة الإلكترونية، واختراق قواعد البيانات، والهدف حماية البيانات من كافة الأساليب غير المشروعة للدخول عليها.

٣- أعلى مستوى إداري أو قيادي :

يتحصر استخدامات مصطلح استراتيجية في كل ما يعمده أو يخططه أو يتداوله المستوى القيادي أو الإداري الأعلى في أية منظمة، ويكون ذلك المستوى هو المسئول عن تحديد وتحقيق غايات المنظمة، وهو المعروف بالمستوى الذي يشترك فيه فريق عمل مكون من جميع قادة الأنشطة بصرف النظر عن حجمها ودورها في التنظيم.

٤ - تخصيص المهام وتحديد المسؤوليات :

كثيراً ما نستخدم مصطلح استراتيجية في حياتنا العامة وحتى العلمية نقلاً عن الغرب دون مراعاة لمذلول هذا المصطلح، فالخطة الاستراتيجية يجب أن ينتج عنها تقسيم للأهداف وتخصيص للمهام وتوزيع للأدوار لمستويات المتوسطة والدنيا، وتبعاً لهذه المهام تمت تلك المستويات خطط جديدة ومنفصلة لتحقيقها والتي بمجموع نجاحها يتحقق الهدف، وإن لم تتواجد تلك الخطط الدنيا فلا مجال لوصف الخطة بالاستراتيجية لفقدتها عنصر تقسيم الأدوار والتعاون وبالتالي فقد القدرة على المناورة.

ومن هذه المعايير نلاحظ أن مصطلح الاستراتيجية لا يفضل استخدامه إلا إذا ارتبط بخطة يضعها أعلى مستوى إداري بالهيكل التنظيمي للمنظمة ويشترط ارتباط الخطة المباشر بتحقيق غايات أو أهداف عامة رئيسية المنظمة ويشترط وجود تهديدات خارجية أو قوة تنافسية مما يستوجب معها استخدام أساليب المناورة أو الاعتماد على تحليل للفرص والتهديدات كما هو في علوم الإدارة، ولا يصح استخدام مصطلح (الاستراتيجية) مع أي موضوع لا تتوافر فيه تلك المعايير سواء على المستوى الإداري أو العلمي.

أهداف استراتيجية أمن المعلومات :

تهدف استراتيجية أمن المعلومات إلى :

- تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الكمبيوتر والشبكات، وكذلك حماية المعلومات بكافة أشكالها، وهي مراحل إدخالها ومعالجتها وتخزينها ونقلها وإعادة استرجاعها.

- تهدف الاستراتيجية إلى تحديد الإلكترونيات التي يتم من خلالها تحقيق وتنفيذ

الفصل الثالث - استراتيجية أمن المعلومات

الواجبات المحددة على كل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر^(١).

- بيان الإجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المناطة بها القيام بها بذلك.

ثالثاً - محل الحماية :

محل الحماية هنا - بصفة أساسية - البيانات فهي الهدف الأساسي لأمن المعلومات، ويتمثل أمن المعلومات في مجموعة من الآليات والإجراءات والأدوات التي تستخدم للوقاية أو للتقليل من المخاطر والتهديدات التي تتعرض لها أجهزة الحاسبات الآلية والشبكات وقواعد البيانات، وهي متعددة من حيث الطبيعة والفرض، ومحور الخطر على المعلومات هو الإنسان، سواء المستخدم أو الشخص المناط به مهام تقنية معينة تتصل بنظام المعلومات، فإدراك هذا الشخص حدود صلاحياته، وإدراكه آليات التعامل مع الخطر، وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية، أو شخص غير مصرح له بالدخول على النظام وقام بعملية اختراق والدخول على نظام المعلومات^(٢).

تتصبب المخاطر والاعتداءات على بيئة وأمن المعلومات في أربع نقاط أساسية، وهي: أمن البيانات والمعلومات، متمثلة في قواعد البيانات المختلفة الموجودة على الشبكة، أمن النظام والتطبيقات والبرامج ونظم التشغيل، الأمن المادي للأجهزة والمكونات المادية، أمن الشبكة والدخول إلى الأنظمة، وهي تشكل مكونات تقنية المعلومات، وكل منها يشمل

(١) يرمن عرب: «الخصوصية وأمن المعلومات»، ورقة عمل مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخليوي - اتحاد المصارف العربية، ٢٠-٢٢ أيار ٢٠٠٦، عمان - الأردن، ٢٠٠٦م.

(2) Karl De Leeuw, J. A. Bergstra : The History of Information Security, A Comprehensive Handbook, Elsevier, 2007, p212.

قواعد ومتطلبات تختلف عن الأخرى ويتعين أن تكون أنظمة الأمن في هذه المواضع متكاملة مع بعضها؛ حتى تحقق الوقاية المطلوبة.

١ - أمن البيانات والمعلومات (أمن قواعد البيانات)؛

وهي تمثل الدم الحي للأنظمة، وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها، وتمتد معناها الواسع للبرمجيات المخزنة داخل النظم، والمعطيات قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وقد تخزن داخل النظم أو على وسائط تخزين خارجية، ويتم اختراق شبكات المعلومات وقواعد البيانات وأجهزة الخدمات الرئيسية للجهات الحكومية أو الشركات بدون تصريح دخول،

٢ - أمن النظام (البرامج والتطبيقات ونظم التشغيل)؛

أمن النظام يقصد به التطبيقات التي يتم التعامل من خلالها على الشبكة وعدم السماح لأشخاص غير مصرح لهم بالدخول على التطبيق، والتطبيقات هي مجموعة من الأوامر التي يتم كتابتها في نسق معين لإنجاز الأعمال، وقد تكون مستقلة عن النظام أو مخزنة فيه ذاته، وتقوم بأعمال محددة، ويقصد بأمن النظام تلك العملية التي يتم من خلالها التأكد من استخدام التطبيق، هل مسموح له بالاستخدام ومدى الصلاحيات الممنوحة له، ويمكن تحديد مستويات الحماية طبقاً لسرية وخطورة البيانات، يمكن تحديد جهاز معين فقط لكل مستخدم، وأيضاً يمكن تحديد ساعات مسمية فقط يستطيع الدخول على التطبيق فيها وخلاف ذلك لا يسمح له باستخدام التطبيق.

٣ - التأمين المادي للأجهزة؛

التأمين المادي للأجهزة، ويقصد به تأمين المكونات المادية للنظام من أجهزة ومعدات من العبث بها ضد السرقة أو التلف، وهي تمثل كافة المعدات والأدوات المادية التي يتكون

منها النظام، كالمشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وكل المكونات المادية للنظام أو الشبكة؛ حيث يتم اختراقها والعبث بما تحويه من معلومات بسهولة اختراقها وعدم وجود الحماية الكافية.

٤ - تأمين شبكة الاتصالات (الولوج أو الدخول إلى الأنظمة) :

محل الحماية لأمن الشبكة هو عملية الاتصال وتبادل البيانات والمعلومات بين أجهزة الحاسب الآلى بالشبكة والنظام النهائي سواء كان نظام المستضيف (الخادم) وبين جهاز حاسب آلى آخر على الشبكة، ويهدف أمن الشبكات توفير وسائل الحماية في تعامله مع الشبكة، وشبكات الاتصال التى تربط أجهزة التقنية بعضها فى بعض محلياً أو دولياً، فتتيح فرصة اختراق النظم من خلالها والتعرف على البيانات والمعلومات أثناء انتقالها من حاسب لآخر أو عند إدخال بيانات سرية فى وثيقة مثل رقم بطاقة الضمان وكلمة السر.

رابعاً - المخاطر المحتملة :

هناك العديد من المخاطر المحتملة التى يمكن أن تواجه نظام المعلومات ويخشى منها، وتتركز تلك المخاطر فى عملية اختراق أمن المعلومات والوصول إلى المعلومات والبيانات بطريقة غير مشروعة وبدون تصريح لذلك عن طريق ثغرات فى نظام الحماية الخاصة بقواعد البيانات أو شبكات الحاسبات، واستغلال تلك نقاط الضعف بسبب القصور فى إجراءات السيطرة والحماية أو من خلال المعلومات التى يجمعها الشخص المخترق من مصادر مادية أو معنوية، كالحصول على كلمات السر أو معلومات عن النظام عن طريق غير مشروع، والقيام بأنشطة غير مصرح له بها، وتلك الثغرات تعد من أهم المخاطر التى تهدد أمن المعلومات؛ حيث لا يمكن ذكر المخاطر على سبيل الحصر، ومن أبرزها ما يلى:

١ - وسائل الأمن المتعلقة بالتعريف بشخص المستخدم ومشروعيته :

هي تلك الأساليب التي تهدف إلى ضمان التحقق من أن الشخص الذي يقوم باستخدام النظام أو الشبكة هو ذلك الشخص المصرح له بهذا الاستخدام وفقاً للصلاحيات الممنوحة له، متمثلة في الدخول على البيانات بالإطلاع أو الإضافة أو التعديل، وذلك من خلال اسم المستخدم وكلمة السر بأشكالها المختلفة، متمثلة في الدخول على النظام أو التطبيقات، والبطاقات الذكية المستخدمة للتعريف بالشخص والسماح له بالدخول إلى أماكن لا يُسمح فيها بالدخول إلا لأشخاص محددين وفي أوقات محددة، أو وسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي كبصمة اليد أو الصوت أو بصمة العين، والمفاتيح المشفرة، والأقفال الإلكترونية التي تحدد دخولها لأشخاص بذاتهم⁽¹⁾.

٢ - الوسائل المتعلقة بالتحكم بالدخول والنفاذ إلى الشبكة :

هذه الوسائل تعمل على الحماية ضد الدخول غير المشروع إلى مصادر الأنظمة والاتصالات والمعلومات، والتأكد من أن الشبكة ومصادرها قد استخدمت بطريقة مشروعة، ويشمل مفهوم الدخول غير المصرح به لأغراض خدمات الأمن الاستخدام غير المصرح به، والتعديل غير المصرح به، والإتلاف غير المصرح به، وإصدار المعلومات والأوامر غير المصرح بها ولهذا فإن خدمات التحكم بالدخول تعد الوسائل الأولية لتحقيق التخويل والتثبت منه.

٣ - مجموعة الوسائل التي تهدف إلى تحقيق سرية المعلومات :

هذه الخدمات تحمي المعلومات من الإفشاء للجهات غير المصرح لها بالحصول عليها، والسرية تعنى بشكل عام إخفاء المعلومات من خلال تشفيرها أو من خلال وسائل

(1) Ohn R. Vacca : Computer and Information Security Handbook, Morgan Kaufmann, C2009, p245.

الفصل الثالث - استراتيجية أمن المعلومات

أخرى كمنع التعرف على حجمها أو مقدارها أو الجهة المرسل إليها، وإجراءات حماية نسخ الحفظ الاحتياطية، والحماية المادية للأجهزة ومكونات الشبكات.

٤ - وسائل الحماية التكاملية :

هذه الخدمات تهدف إلى حماية مخاطر تغيير البيانات وضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخولة بذلك، أثناء عمليات إدخالها أو معالجتها أو نقلها وعمليات التفسير. تعنى بمفهوم الأمن هنا الإلغاء أو التحويل أو إعادة تسجيل جزء منها أو غير ذلك وتهدف هذه الوسائل أيضاً إلى الحماية من أنشطة تدمير المعطيات بشكل كامل أو إلغائها دون تخويل باستخدام برامج الكشف عن الفيروسات^(١).

٥ - إنكار الخدمة :

يتم ذلك من خلال القيام بأنشطة تمنع المستخدم الشرعي من الوصول إلى المعلومات أو الحصول على الخدمة وأبرز أنماط إنكار الخدمة إرسال كمية كبيرة من رسائل البريد الإلكتروني دفعة واحدة إلى موقع معين بهدف إسقاط النظام المستقبل لعدم قدرته على احتمائها أو توجيه عدد كبير من عناوين الإنترنت على نحو لا يتيح عملية تجزئة حزم المواد المرسله فتؤدي إلى اكتظاظ الخادم وعدم قدرته على التعامل معه.

٦ - عدم الإقرار بالقيام بالتصرف :

يتمثل هذا الخطر في عدم إقرار الشخص المرسل إليه أو المرسل بالتصرف الذي صدر عنه، كأن ينكر أنه ليس هو شخصاً الذي قام بإرسال طلب الشراء عبر الإنترنت، وتهدف هذه الوسائل إلى ضمان عدم قدرة شخص المستخدم من إنكار أنه هو الذي

(1) Paulus R. Wayleith: Data Security: Laws and Safeguards, Nova Science Publishers, C2008, p76.

قام بالتصريف، وهي وسائل ذات أهمية بالغة في بيئة الأعمال الإلكترونية والتعاقدات على الخط، وترتكز هذه الوسائل في الوقت الحاضر على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة عن طرف ثالث.

٧- وسائل مراقبة الاستخدام وتتبع سجلات النفاذ :

وهي التقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بالعمل المعين في وقت معين، وتشمل كافة أنواع الهرمجات والسجلات الإلكترونية التي تحدد الاستخدام.

٨- الاعتداء على حق التحويل :

يتم ذلك من خلال قيام الشخص المخول له استخدام النظام لفرض ما باستخدامه هي غير هذا الغرض دون أن يحصل على التحويل بذلك، وهذا الخطر يعد من الأخطار الداخلية، إساءة استخدام النظام من قبل موظفي المنشأة، وقد يكون أيضاً من الأخطار الخارجية، كاستخدام المخترق حساب شخص مخول له باستخدام النظام عن طريق تخمين كلمة السر الخاصة به أو استغلال نقطة ضعف بالنظام للدخول إليه بطريق مشروع أو من جزء مشروع ومن ثم القيام بأنشطة غير مشروعة^(١).

٩- زراعة نقاط الضعف :

عادة ينتج هذا الخطر عن افتحام من قبل شخص غير مصرح له بذلك أو من خلال مستخدم مشروع تجاوز حدود التحويل الممنوح له بحيث يقوم الشخص بزرع مدخل ما يحقق له الاختراق فيما بعد، ومن أشهر أمثلة ذلك زراعة المخاطر حصان طروادة، وهو عبارة عن برنامج يؤدي غرضاً مشروعاً في الظاهر لكنه يمكن أن يستخدم في

(1) L.Jean Camp, Stephen Lewis: Economics of Information Security, Springer, C2004, p163.

الفصل الثالث - استراتيجية أمن المعلومات

الخفاء للقيام بنشاط غير مشروع، كان يستخدم برنامج معالجة كلمات ظاهرياً لتحرير وتنسيق النصوص في حين يكون غرضه الحقيقي طباعة كافة ملفات النظام ونقلها إلى ملف مخفي بحيث يمكن للمخترق أن يقوم بطباعة هذا الملف والحصول على محتويات النظام.

١٠ - مراقبة الاتصالات :

بدون اختراق كمبيوتر المجنى عليه يتمكن الجاني من الحصول على معلومات سرية غالباً ما تكون من المعلومات التي تسهل له مستقبلاً اختراق النظام وذلك ببساطة من خلال مراقبة الاتصالات من إحدى نقاط الاتصال أو حلقاتها.

١١ - اعتراض الاتصالات :

كذلك بدون اختراق النظام يقوم الجاني في هذه الحالة باعتراض المعطيات المنقولة خلال عملية النقل ويجري عليها التعديلات التي تتناسب مع غرض الاعتداء ويشمل اعتراض الاتصالات قيام الجاني بخلق نظام وسيط وهمي بحيث يكون على المستخدم أن يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي^(١).

خامساً - أهم أساليب تأمين قواعد البيانات :

تأمين قواعد البيانات والحفاظ عليها من المخاطر السابق الحديث عنها، ومنع الدخول غير المشروع إلى شبكات الحاسب، والوصول إلى أجهزة الشركة دون رغبتهم أو علمهم، بالإضافة إلى الأضرار المادية والمعنوية الجسيمة التي قد يحدثها عند إتلافه أو الإطلاع أو سرقة بيانات أو ملفات أو صور خاصة.

هناك عدة أساليب لتأمين قاعدة البيانات تتمثل في البرمجيات المختلفة للحفاظ

(1) Tyler Moore: *Economics of Information Security and Privacy*, Springer, C2010, p127.

على معلوماتك آمنة، كاستخدام برمجيات لمكافحة الفيروسات والاختراقات، وأيضاً استخدام برامج أو أجهزة الجدار النارية لمنع من الاختراق، بالإضافة إلى الأساليب التقنية في المحافظة على البيانات والمعلومات وسلامة المحتوى بإتباع أسلوب التشفير، وسنتناول أهمها على النحو التالي:

أ- برمجيات كشف ومقاومة الفيروسات :

هي البرامج التي تقوم بحماية الأجهزة من هجمات الفيروسات التي تشكل تهديداً أمنياً على أمن البيانات، يمكنها رصد مصدر هذه البرامج في القرص الصلب أو الأقراص المدمجة، أو وحدات الحفظ الخارجي، أو الرسائل الإلكترونية، هي حالة اكتشاف الفيروس تعمل هذه البرمجيات على مسح أو تعطيل عمله.

وتعد تقنيات مضادات الفيروسات الأكثر انتشاراً، إلا أن هناك ثغرات هي فهم دور هذه المضادات للفيروسات التي تصيب النظام، وما قد ينتج من الاستخدامات الخاطئة لها على أداء وفعالية النظام، وسنتعرض لمأهية الفيروسات، والبرامج الخاصة بمكافحة الفيروسات، ونشأتها، وكيفية عملها.

ما هي الفيروسات

فيروس الحاسب الآلي هو عبارة عن برنامج صغير يتم إدخاله على الحاسب الآلي بدون علم المستخدم وتسبب أمور غير متوقعة وأشياء ضارة وغير مرغوبة بفرض تدمير بعض أو جميع البرامج والأجهزة المكونة للحاسب الآلي، أو لتسهيل عملية الدخول غير المشروع للنظام^(١). يقوم من أنشأ الفيروس ببرمجته وتوجيه الأوامر الخاصة له بتحديد التوقيت الذي يبدأ فيه الفيروس بالنشاط وعادةً ما تعطى فرصة كافية من الوقت

(١) أشرف السعيد أحمد : مقدمة في علوم الحاسب للتعلم، ٢٠١١م ص ١٦٦.

الفصل الثالث - استراتيجية أمن المعلومات

للفيروس؛ حتى يضمن حرية الانتشار دون أن يلتفت الانتباه ليتمكن من إصابة أكبر عدد ممكن من الملفات في النظام، تختلف الفيروسات من حيث بدأ النشاط فهناك من يبدأ بتاريخ أو وقت محدد، وهناك من يبدأ بالعمل بعد تنفيذ أمر معين في البرنامج المصاب وهناك من يبدأ بالنشاط بعد التكاثر والوصول إلى رقم معين من النسخ، وبعد أن ينشط الفيروس يقوم الفيروس بعدة أنشطة تخريبية حسب الغرض من إنشاء ذلك الفيروس، فهناك من يقوم بعرض رسالة تستخف بالمستخدم أو تقوم بعرض رسالة تحذيرية عن امتلاء الذاكرة وهناك أنواع أخرى تقوم بحذف أو تعديل بعض الملفات، وهناك من يقوم بتكرار ونسخ نفسه؛ حتى يشل جهازك تماماً وأنواع أخرى تقوم بمسح كل المعلومات من القرص الصلب.

البرامج المضادة للفيروسات (Virus countermeasures) :

برامج مكافحة الفيروسات هي البرامج التي تستخدم لحماية الأجهزة من هجمات الفيروسات ويقية البرامج التي تشكل تهديداً أمنياً على المعلومات، وتستطيع أن تحدد هذه الملفات الضارة القادمة من أي مصدر مثل الأقراص المدمجة والأقراص اللينة والرسائل الإلكترونية وكذلك يمكنها رصد هذه البرامج في القرص الصلب، وتسميتها بمضادات الفيروسات لا يجعلها قاصرة على مكافحة الفيروسات فقط، بل هو اصطلاح يطلق على هذا النوع من البرمجيات. وفي كثير من الأحيان يطلق على كل البرامج الضارة اسم فيروس بغض النظر عما إذا كان فيروس فعلاً أو دودة أو (Trojan Horse) أو أي نوع آخر من أنواع البرمجيات الضارة⁽¹⁾.

وتتمكن هذه البرامج من مسح أو تعطيل عمل البرامج المهددة لسلامة الجهاز وملفات البرامج الموجودة على جهاز الحاسب ويتكون برنامج مضاد الفيروسات من

(1) Tyler Moore, Op.Cit, P145.

جزئين مختلفين:

١- التشغيل المباشر عند الدخول :

وهذا الجزء يعمل تلقائياً عند تشغيل (الدخول) للبرامج أو تحميل الملفات من الإنترنت وهو ما يعرف (On Access Element) .

٢- التشغيل عند الطلب :

وهذا الجزء يعمل عندما تطلب أنت منه ذلك، وهو متخصص بالكشف عن الفيروسات وأحصنة طروادة (TORJAN) فى القرص الصلب والأقراص اللينة والأقراص المدمجة وهو ما يُعرف (Demand Element).

هناك تسابق مستمر بين مطوري البرامج الضارة وبرامج مضادات الفيروسات، فكلما وجد برنامج فعال لمكافحة الفيروسات الحالية، يتم إنتاج نوع جديد من الفيروسات لا يعالجها البرنامج الحالى.

العلاج الناجح للفيروسات هو منعها أو عدم السماح لها بالدخول لنظام الحاسب إلا أن تحقيق ذلك يعد من الصعوبة بمكان، ولكن إذا حدث الإصابة بالفيروس فهناك إجراءات يمكن اتخاذها فى مواجهة الفيروس أو معالجته وتقليل عواقبه وهى عبارة عن خيارات يتم اختيار الأنسب منها والذي يوفر أعلى حماية وأقل تكلفة^(١).

نشأة برمجيات مكافحة الفيروسات :

عقب ظهور الفيروسات كانت بداية قيام بعض الشركات فى تصميم برامج مكافحة الفيروسات لحماية أجهزة الحاسب الألى، ومع السباق السريع فى تصميم وتطوير الفيروسات التى كانت بسيطة فى بداية ظهورها، أصبح هناك تعقيداً كبيراً طرأ على

(1) Karl De Leeuw, J. A. Bergstra, Op.Cit, P95.

الفصل الثالث - استراتيجية أمن المعلومات

برامج مكافحة الفيروسات لمواجهة تطور الفيروسات بشكل سريع، ويمكن تقسيم المراحل والأجيال التي تطورت خلالها برامج مكافحة الفيروسات إلى ما يلي:

الجيل الأول - المسحات البسيطة (Simple Scanner)،

كانت بداية ظهور برمجيات مكافحة الفيروسات مع أول ظهور للفيروسات بسيطة نظرًا لبساطة الفيروسات وسهولة التعرف عليها وكانت تلك البرمجيات كانت تعتمد على بعض النقاط البسيطة وغير المعقدة لاكتشاف الفيروسات والقضاء عليها وتعتمد تلك البرامج في هذه المرحلة على ما يلي:

- يحتاج برنامج مكافحة الفيروسات علامة معينة (Signature) للتعرف من خلالها على الفيروس.

- في بعض أنواع برنامج مكافحة الفيروسات يتم الاعتماد على قياس حجم الملف واكتشاف التغير في الطول نتيجة التصاق الفيروس به^(١).

الجيل الثاني - المسحات الموجهة (Heuristic Scanner)،

وهي تتميز بالآتي:

- استخدام طرق موجهة للبحث عن الإصابات المتوقعة.

- بعضها يبحث عن كود فيروسي معين داخل الملفات فإذا وُجد؛ فهذا يعني إصابة الملف المحدد.

- ويمكن -أيضًا- اختبار صحة الملفات (Integrity) باستخدام قيمة الـ (Checksum) الموجودة مع الملفات فإذا كان الفيروس قد غيّر الملف دون أن يُعدل قيمة الـ (Checksum) فإن البرنامج المضاد للفيروسات سيكتشف

(١) أشرف المسعود أحمد - مقدمة في علوم الحاسب - مرجع سابق، ص ١٦٦.

أن هناك إصابة، نسبة لاختلاف قيمة (Checksum) المخزنة مع بيانات الملف⁽¹⁾.

الجيل الثالث - الماسحات البسيطة (Activity Trap).

في تلك النوعية من البرمجيات يتم اكتشاف فيروسات الذاكرة بالأفعال التي تقوم بها في النظام وليس بتركيبها كما في الجيل السابق.

الجيل الرابع - الحماية الكاملة (Full-featured protection).

هذا الجيل من التقنية تستخدم كل التقنيات السابقة في حزمة واحدة وتحتوي مقدرات كبيرة تحد من انتشار الفيروسات ونشاطها التخريبي.

كيفية عمل البرامج المضادة للفيروسات :

البرامج المضادة للفيروسات عبارة عن تقنية مسح ورصد للبرامج المشبوهة التي تتميز بخصائص معينة أو تحتوي على صيغة معينة من البرمجة عبارة عن مجموعة من الأرقام الثنائية وهي التي تعرف بـ (التوقيع) ويتم ذلك بالطريقة التالية:

يقوم البرنامج المضاد بتحديد كل الملفات والبرامج ذات الطبيعة التنفيذية، ويتم مقارنة التوقيع الموجود على كل ملف بالتواقيع المخزنة في قاعدة المعلومات الخاصة بالبرنامج المضاد للفيروسات، بعد عملية المقارنة يقوم البرنامج المضاد باكتشاف الفيروس أو حصان طروادة ويقوم بإخطار المستخدم عنه، يقوم البرنامج المضاد بتنخير المستخدم بين مسح أو تعطيل الفيروس أو بإصلاح الخلل بطريقة آلية، ويتم ذلك من خلال مرحلتين :

(1) Karl De Leeuw, J. A. Bergstra, Op.Cit, P144.

المرحلة الأولى - اكتشاف الفيروس (Virus Detection)؛

هي تحديد حدوث الإصابة بالفيروس وتحديد مكانه، ويتم التعرف على نوع الفيروس الذي سبب الإصابة (Identification) عقب اكتشاف الإصابة، وذلك من خلال علامات معينة في كود الفيروس أو سلوكه الذي يقوم به في النظام؛ حيث يقوم مصنعو ومبرمجو الفيروسات - عادةً - بتعديل أو تحريف التوقيع الأصلي لبعض البرامج الشهيرة وذلك لتضليل المستخدم والبرنامج الأصلي وتقوم تكنولوجيا الكشف من هذا التزوير والتعديل بواسطة المقارنة السريعة بين التوقيعات الأصلية والمزيفة.

المرحلة الثانية - إزالة الفيروس (Virus Removal)؛

بعد التعرف على نوع الفيروس تتم إزالته من الملف المصاب وإرجاع الملف إلى وضعه الأصلي وتُعقَّب كل النسخ الأخرى من الفيروس للحد من انتشاره مرةً أخرى، إذا أسفرت مرحلة الاكتشاف عن وجود فيروس لم يتم التعرف على نوعه يجب اللجوء لخيار التخلص من البرنامج المصاب، ثم إعادة تركيبه مرةً أخرى باستخدام النسخ الاحتياطية.

مفاهيم خاطئة عن برامج الحماية من الفيروسات؛

لعل من أكثر المفاهيم الخاطئة بين المستخدمين على مستوى العالم هي الاعتقاد بأن اقتناء برنامج مضاد للفيروسات يمنع ويحمي من هجومات الهاكرز والمخترقين وهذا طبعاً ليس صحيح؛ حيث إن هذه البرامج تحمي فقط من الفيروسات والديدان وتستطيع التعرف على معظم أحصنة طروادة ولكن لا تقوم بفلق المنافذ والمعايير الموجودة في جهاز الحاسب الآلي والتي تمكن المخترقين من الوصول إلى الجهاز والمعلومات.

مدى الاعتمادية على هذه البرامج :

ليس هناك برنامج مضاد للفيروسات قادر على تقديم حماية كاملة لجهاز الحاسب الآلى، وعند القيام بالتحديث المستمر لبرنامج مكافحة الفيروسات -بصفة مستمرة- سوف تحصل على حماية تصل إلى ٩٥٪، لظهور أنواع جديدة من الفيروسات لم يتمكن البرنامج من اكتشافها؛ حيث تعمل هذه البرمجيات بأسلوب رد الفعل -دائمًا- الفيروسات تتقدم بالجديد ويأتى التحديث لمحاولة اكتشاف تلك الفيروسات والقضاء عليها.

ب- الجدار الناري (Fire Wall) :

هى عبارة عن أجهزة (Hardware)، أو برامج (Software)، وتعمل على فلترة وتصفية حركة البيانات الواردة والصادرة من وإلى الشبكة اعتمادًا على قوانين ومعاملات بسيطة، وتطورت الجدران النارية بشكل كبير منذ نشأتها، ويمد أول استخدام لها لتحقيق الأمن فى أوائل التسعينات، وكان عبارة عن موجهات لبروتوكول (IP) للتحقق من هوية المستخدمين، باستخدام أسلوب اسمح للمستخدم الفلانى بالدخول والنفاذ إلى الملف التالى، أو أمنع المستخدم فلان (أو برنامج معين) من الدخول إلى المنطقة (أو المناطق) التالية^(١).

وكانت هذه الجدران النارية فعالة ولكنها محدودة؛ حيث كان من الصعب فلترة البيانات، وتحديد أجزاء التطبيقات المراد منعها من النفاذ إلى الشبكة، وهى أحيان أخرى كانت عناصر الشبكة، مثل الموظفين العاملين ضمنها، تتغير، مما كان يستدعى تغيير القوانين، وجاءت الأجيال التالية من الجدران النارية أكثر قدرة وأكثر مرونة للتعديل وأدى ذلك إلى المزيد من الابتكارات، ليس فقط فى مجال تسريع أداء الجدران

(1) Kimberly Kiefer: Information Security: A Legal, Business, and Technical Handbook, American Bar Association, C2004, p37.

الفصل الثالث - استراتيجيات أمن المعلومات

النارية وتقديم خدماتها، بل وأيضاً في تضمينها قدرات متعددة في التعامل وإجراء التعديلات المطلوبة، وتمثل هذه القدرات في ما يلي⁽¹⁾:

١ - التحقق من هوية المستخدمين :

بداية التطوير في الجدران النارية كان من حيث القدرات القوية للتحقق من الهوية، وإذا كانت السياسات الأمنية التي تتبعها المؤسسة تسمح بالنفاذ إلى الشبكة من شبكة خارجية مثل الإنترنت، فظهرت الحاجة إلى استخدام أسلوب للتحقق من هوية المستخدمين، ويقصد بالتحقق من الهوية هو التأكد من صحة شخصية المستخدم بشكل يتجاوز مجرد التحقق من اسم المستخدم والكلمات السرية والتي لا تعتبر بحد ذاتها وسيلة قوية للتحقق من هوية المستخدمين؛ حيث إن أسماء المستخدمين وكلماتهم السرية يمكن نسخها وإعادة استخدامها، أما الأساليب القوية للتحقق من هوية المستخدمين فتستخدم أساليب التشفير مثل الشهادات الرقمية، أو برمجيات حساب الشفرات الرقمية الخاصة، وبواسطة الشهادات الرقمية يمكن تقاضى هجمات إعادة الاستخدام؛ حيث يتم نسخ اسم المستخدم وكلمته السرية وإعادة استخدامها للنفاذ إلى الشبكة.

٢ - وسائل مراقبة الاستخدام وتتبع سجلات الدخول والخروج للشبكة (Logging and Monitoring) :

وهي التقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بعمل معين في وقت محدد، ومراقبة العمليات التي قام بها هذا الشخص، وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الاستخدام مثل (Log File) و(Edit Records)، تشمل أيضاً برامج مراقبة الشبكة، وهي تعد إضافة كبيرة للجدار النارية والاختراقات.

(1) Indira Carr, Computer Crime International Library ■ Criminology, Criminal Justice and Penology- Second Series Ashgate,, C2009, P167.

٣ - الشبكات الافتراضية الخاصة (Virtual Private Networks) :

وتعد الإضافة الثالثة إلى الجدران النارية هي التشفير البيئي للجدران النارية (Firewall-to-Firewall) والتي تعرف بالشبكات الافتراضية الخاصة (Virtual Private Networks)، وسميت هذه الشبكات بالخاصة لأنها تستخدم التشفير، وسميت بالافتراضية الخاصة لأنها تستخدم الإنترنت وشبكات عامة لنقل المعلومات الخاصة.

رغم أن الشبكات الافتراضية الخاصة كانت متوفرة قبل برمجيات الجدران النارية باستخدام الموديمات (Modems) والموجهات (Routers) للتشفير لكنها أصبحت تستخدم فيما بعد ضمن برمجيات الجدران النارية، وهي جيل جديد من الجدران النارية يحتوي على عدد من التقنيات بما في ذلك حلول جدران نارية جاهزة، بمعنى أنها لا تحتاج إلى إعداد من قبل المستخدم ويمكن البدء باستخدامها فور الحصول عليها دون الحاجة إلى إجراء أية تعديلات خاصة على نظام التشغيل أو البنية التحتية المستخدمة، وانتقلت وسائل حماية الإنترنت من مستويات الحماية الفردية، التي تقوم على وضع وسائل الحماية ومنها الجدران النارية في المنطقة التي تفصل الشبكة الخاصة عن الموجهات التي تنقل الاتصال إلى الشبكة العالمية (الإنترنت)، إلى مستويات الأمن المتعددة والتي تقوم على فكرة توفير خطوط إضافية من الدفاع بالنسبة لنوع معين من المعلومات أو نظم المعلومات داخل الشبكة الخاصة، وتعتمد وسائل الأمن متعددة الاتجاهات والأغراض آليات مختلفة لتوفير الأمن الشامل للنظام⁽¹⁾.

٤ - مراقبة المحتوى (Content Screening) :

يقصد به تحليل محتويات الحزم (Packets) الواردة للشبكة ومعرفة واختبار محتواها، وخلال الأعوام القليلة الماضية أصبح من الشائع استخدام الجدران النارية كأدوات لمراقبة

(1) Kimberly Kiefer, Op.Cit, P54.

المحتوى الوارد إلى الشبكة للبحث عن الفيروسات والبرمجيات الضارة، ومراقبة عناوين الإنترنت.

أهمية استخدام الجدار الناري:

تقوم أجهزة وبرمجيات الجدار الناري بالعمل على حماية وعزل التطبيقات والخدمات والأجهزة من الشبكة الداخلية من حركة المرور غير المرغوب فيها القادمة من الإنترنت العامة، والحد من أو تعطيل الوصول من المضيفين من الشبكة الداخلية لخدمات الإنترنت العامة، كما -أيضاً- تعمل على دعم ترجمة عنوان الشبكة (NAT)، والذي يسمح للشبكة الداخلية لاستخدام عناوين (IP) الخاصة ومشاركة اتصال واحد على شبكة الإنترنت العامة (إما مع عنوان (IP) واحد أو مجموعة مشتركة من العناوين العامة تمييزه تلقائياً).

ويعد تركيب جدار حماية ناري أكثر الطرق فاعلية، وأهم خطوة أولية يمكنك اتخاذها لحماية جهاز الحاسب الآلي قبل الدخول إلى الإنترنت للمرة الأولى، وتختلف الجدران النارية حسب احتياجات المستخدم، فإذا استدعت الحاجة إلى وضع جدار النار على عقدة منفردة عاملة على شبكة واحدة فإن جدار النار الشخصي هو الخيار المناسب. وفي حالة وجود حركة مرور داخلية وخارجية من عدد من الشبكات، فيتم استخدام مصافي لجدار النار في الشبكة لتصفية جميع الحركة المرورية، وكثير من الشبكات والخوادم تأتي مع نظام جدار نار افتراضي، ولكن ينبغي التأكد فيما إذا كان يقوم بعمل تصفية فعالة لجميع الأشياء التي تحتاج إليها، فإن لم يكن قادراً على ذلك، فينبغي توفير جدار حماية ناري أقوى منه، وبعض أنظمة التشغيل تحتوي على حماية ناري، مثل ويندوز اكس بي مع الحزمة الخدمية/الإصدار 2 (Service Pack2) ونظام التشغيل ماكنتوش (MacOS X).

ج - التشفير (Encryption) :

يعرف التشفير بأنه عملية ترميز البيانات وتحويل المعلومات إلى شفرات غير مفهومة تبدو غير ذات معنى ليتعذر قراءتها من أي شخص غير المرخص لهم من الاطلاع على تلك البيانات والمعلومات أو فهمها، أي أنها عملية الحفاظ على سرية البيانات والمعلومات باستخدام برامج لها القدرة على تحويل وترجمة تلك البيانات والمعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يمكنهم فهم أي شيء لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة، على اختلاف أنواع وأشكال البرامج المتخصصة في هذا المجال إلا أنها جميعاً تتشارك في القاعدة أو الأساس وهي مبنية على مفهوم بسيط؛ حيث يقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس، ويجعل التشفير المعلومات في جهاز الحاسب الآلي غير قابلة للقراءة من قبل أي شخص يستطيع أن يتصل بخلسة إلى الجهاز دون إذن، ويتم ذلك باستخدام بروتوكول تشفير الشبكات اللاسلكية (WEP) ⁽¹⁾.

وتحظى تقنيات وسياسات التشفير باهتمام كبير في مجال أمن المعلومات؛ حيث تمثل حماية التشفير الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة، السرية، التكاملية، توفير المعلومات، فالتشفير يعمل على تحقيق توفير وحماية هذه العناصر، فضمان سرية المعلومات أصبح يعتمد على تشفير وترميز الملفات والمعطيات، بل تشفير وسائل التحقق من المستخدم، وكلمات السر، كما أن وسيلة حماية سلامة المحتوى تقوم على تشفير البيانات المتبادلة والتأكد لدى فك التشفير أن الرسالة الإلكترونية لم تتعرض لأي نوع من التعديل أو التغيير، ويعد التشفير بوجه عام وتطبيقاته المديدة، من أهم الوسائل لضمان عدم إنكار التصرفات عبر الشبكات الإلكترونية.

(1) Karl De Leeuw, J. A. Bergstra, Op.Cit. P164.

الفصل الثالث - استراتيجية أمن المعلومات

والتشفير يتم من خلال مرحلتين رئيسيتين، المرحلة الأولى تتمثل في تشفير النص على نحو يحوله إلى رموز غير مفهومة، أو رموز مقروءة بلغة غير مفهومة، والمرحلة الثانية تتم عقب استلام الرسالة وتتمثل في فك الترميز بإعادة النص المشفر إلى وضعه السابق كنص مفهوم ومقروء، وهذه المسألة تقوم بها برمجيات التشفير التي تختلف أنواعها ووظائفها⁽¹⁾.

أنواع تكنولوجيا التشفير

هناك نوعان من التكنولوجيا المستخدمة في التشفير وهي التشفير المتناظر والتشفير غير المتناظر (Symmetric Algorithms and Asymmetric Algorithms).

والفرق بينهما بسيط جدًا ولكنه مهم جدًا في مستوى ودرجة الأمن؛ حيث إن التشفير المتناظر يتم بتشفير الرسالة أو المعلومات باستخدام الرقم العام وكذلك في الوقت نفسه يتم فك الشفرة وترجمة المعلومات إلى وضعها الأصلي باستخدام الرقم العام نفسه⁽²⁾.

وبذلك لو كان هناك شخص آخر يعرف هذا الرقم أو حصل عليه من الدليل العام فإنه قادر على فك الشفرة وقراءة تلك الرسالة أو المعلومة، أما إذا ما تم تشفير المعلومات بأسلوب (غير المتناظر) فإن المعلومات يتم تشفيرها بالرقم العام ولكن لا يمكن فك الشفرة والوصول إلى تلك المعلومات إلا بالمفتاح الخاص لصاحب ذلك المفتاح العام الذي تمت على أساسه عملية التشفير، أما من حيث طرق التشفير، فثمة التشفير الترميزي، والتشفير المعتمد على مفاتيح التشفير، التي قد تكون مفاتيح عامة أو خاصة أو مزيجًا منها.

(1) Paulus R. Wayleith, Op .Cit, P94.

(2) Ohn R. Varca, Op.Cit, P97.

ويتم تطبيق هذا المبدأ في مجال التشفير من خلال إصدار رقم الأساس عن طريق البرنامج المخصص أو إحدى الهيئات المستقلة والمتخصصة في إصدار هذه الأرقام وهو ما يعرف بـ (Certificate Authority) (CA)، بحيث يكون لكل مستخدم رقم أساس وهو (ع) ويتم تقسيم هذا الرقم إلى مجموعتين (س) وهو ما يعرف بالمفتاح العام و(ص) هو ما يعرف بالمفتاح الخاص، بحيث إذا قمنا بعملية ضرب (س X ص) يكون الناتج هو (ع) الرقم الأساس وهو الرقم اللازم لإعادة الملفات والمعلومات إلى وضعها الأصلي قبل التشفير وطبعاً هذا الرقم محمي ومشفر بقوة ولا يمكن الوصول إليه بسهولة.

المفتاح العام (Public Key) :

المفتاح العام هو ذلك الرقم الذي يتم تداوله ونشره بين بقية المستخدمين لتشفير أية معلومات أو رسالة إلكترونية مخصصة ويعتبر رقمك العام أساس عملية التشفير ولا يستطيع أحد فك رموز تلك المعلومة غيرك أنت، لأنها تحتاج إلى الرقم السري وليكن هو المفتاح الخاص بك لإكمال العملية الحسابية والوصول إلى الرقم الأساس وبالتالي فتح الملفات مرة أخرى.

المفتاح الخاص (Private Key) :

المفتاح الخاص هو النصف الآخر المكمل للمفتاح العام للوصول إلى الرقم الأساس وإعادة المعلومات المشفرة إلى وضعها الطبيعي قبل التشفير، وهذا المفتاح هو الذي يميز كل شخص عن غيره من المستخدمين ويكون بمثابة هوية إلكترونية تمكن صاحبها من فك أية معلومة مشفرة مرسلة إليه على أساس رقمه العام ولذلك يجب عليك الاحتفاظ بالمفتاح الخاص سراً، وبهذه الطريقة لا يستطيع أحد فك الشفرات وقراءة المعلومات المحمية بهذه الطريقة دون اكتمال الحلقة والتي لا تتم إلا بمعرفة القيمة الصحيحة للمفتاح العام والمفتاح الخاص.

الفصل الرابع

تكنولوجيا المعلومات الأمنية
والحكومة الإلكترونية

الفصل الرابع تكنولوجيا المعلومات الأمنية والحكومة الإلكترونية

تمهيد:

تعد وزارة الداخلية من أولى الوزارات التي أخذت بنهج التطور الإلكتروني والتحول من الإدارة التقليدية إلى الإدارة الإلكترونية بل والتقدم والتطور في هذا المجال لتصبح من الركائز الأساسية لنجاح الحكومة الإلكترونية في مصر، وتعد الإدارة الإلكترونية في وزارة الداخلية من أجد المحركات الأساسية والفعالة في إدارة الحكومة الإلكترونية المصرية، وتقدم وزارة الداخلية خدماتها عبر الموقع الخاص بوزارة الداخلية على شبكة الإنترنت العالمية، بالإضافة إلى بعض الخدمات على موقع بوابة الحكومة الإلكترونية المصرية التي تُبث عبر شبكة الإنترنت.

وفي ضوء ما تقدم، سنتناول هذا الموضوع على النحو الآتي :

أولاً ، مفهوم الحكومة الإلكترونية.

ثانياً ، تطبيقات وزارة الداخلية المصرية في مجال الحكومة الإلكترونية.

ثالثاً ، تكنولوجيا المعلومات الأمنية في مجال تيسير وتبسيط إجراءات حصول المواطنين على الخدمات الأمنية الجماهيرية.

أولاً - مفهوم الحكومة الإلكترونية :

يتسم العمل الحكومي في معظم دول العالم بإجراءاته الروتينية الطويلة وبالبطء العام، وهذا يُشكل تكلفة كبيرة على الدول من حيث الجهد المبذول، وعدم استغلال الموارد المتاحة على الوجه الأمثل، ومع تطور التقنيات الحديثة وثورة المعلومات اتجه العالم بأكمله نحو تبني الوسائل الحديثة المتمثلة في استخدام تكنولوجيا المعلومات والاتصالات وخصوصاً الإنترنت للوصول إلى حكومات أفضل.

ويعد مفهوم الحكومة الإلكترونية أحد الطرق الحديثة والمتطورة التي تتعامل بها حكومات الدول لاستخدام التقنية الحديثة في تحسين كفاءة المؤسسات والأجهزة الحكومية واستغلال الموارد المتوفرة داخل الدولة بالشكل الأفضل، لتزويد المواطنين بآليات أفضل وأسرع وأيسر للوصول إلى المعلومات والخدمات داخل مؤسسات الدولة والعمل على توحيد المعلومات الحكومية وترتيبها وتنظيمها، وتتيح للمواطنين المشاركة بأرائهم ومقترحاتهم لدى المؤسسات الحكومية.

وتعرف الحكومة الإلكترونية بأنها «استخدام تكنولوجيا الاتصالات والمعلومات لتحقيق الإصلاح من خلال تسريع عملية الشفافية، وتقريب المسافات، وإزالة العوائق، وإعطاء الفرصة للمواطنين للمشاركة في كافة مراحل العملية السياسية والقرارات المتعلقة بها والتي تؤثر على نواحي حياتهم المختلفة»^(١).

أهداف برنامج الحكومة الإلكترونية:

لا يقتصر مفهوم الحكومة الإلكترونية على كونه تغييراً في أسلوب العمل يتم بمقتضاه إجراء المعاملات نفسها بصورة إلكترونية، ولكنه يشكل نمطاً وشكلاً جديداً للحكومة بمفهومها التقليدي من خلال تبسيط الإجراءات وتحسين الخدمات الحكومية وإعادة

(١) رأفت رضوان : الحكومة الإلكترونية، القاهرة، المركز الدولي للدراسات المستقبلية والاستراتيجية، ٢٠٠٥م، ٢٢ ص.

تنظيم الأجهزة الحكومية، وتسهيل الوصول إلى الخدمات الحكومية عن طريق إتاحة عدد كبير من الخدمات الحكومية عبر بوابة الحكومة المصرية، وعبر قنوات جديدة مثل شبكات الهاتف المحمول، مراكز الاتصال، منافذ الخدمات الجماهيرية والشبكات الواحد، والعمل على توفير خدمات حكومية جديدة.

تبسيط الإجراءات عن طريق إجراءات إصدار التصاريح (المباحية، الصناعية، المحاكم ... إلخ)، وصميم الخدمات الحكومية من منظور المواطن، إتاحة خدمة التوقيع الإلكتروني، تقديم وسائل جديدة لسداد الرسوم مثل (بطاقات الائتمان، السداد عند التسليم، عن طريق الهاتف المحمول وخلافه).

دعم شفافية الجهات الحكومية عن طريق نشر نتائج التوظيف، ميكنة إجراءات إصدار التصاريح، وإرسال إخطارات إلى بوابة المشتريات الحكومية عن طريق الهاتف المحمول.

ومن أهم أهداف الحكومة الإلكترونية ما يلي^(١):

١ - تقديم الخدمات إلى المواطنين في مكان وجودهم :

تمد تقديم الخدمات الجماهيرية للمواطنين في أماكن تواجدهم من أهم أهداف الحكومة الإلكترونية والتي تسعى إلى زيادة قدرة الحكومة على توفير المعلومات والخدمات العامة للمستفيدين بتكلفة أقل، وسرعة ودقة في إنجاز المعاملات وخدمات الجمهور، بطريقة متواصلة ومفيدة للمواطنين بالشكل والأسلوب المناسبين مع تطوير أفضل الطرق لمشاركتهم في العملية التنفيذية، ويتم التعامل الإلكتروني في الخدمات الحكومية من خلال ميكنة هذه الخدمات بصورة تحقق إمكانية الحصول على الخدمات

(١) فريد النجار: الحكومة الإلكترونية، بين النظرية والتطبيق، الإسكندرية، الدار الجامعية، ٢٠٠٨، ص ٢٤١.

دون الحاجة إلى الانتقال إلى مقر أداء الخدمة من خلال^(١):

- التعرف على إجراء ومتطلبات الحصول على الخدمة.

- إتاحة وتوفير النماذج المستخدمة في أداء الخدمة.

- فتح قناة اتصال بين الأفراد والجهات الحكومية.

٢- تحسين أداء المؤسسات الحكومية من خلال ما يلي :

- تخفيض الإنفاق الحكومي والتكاليف المباشرة عن طريق الاستخدام الأمثل للموارد واستحداث آليات جديدة، وخفض تكلفة الخدمات بصورة فعالة^(٢).

- الانفتاح على العالم الخارجى وتوفير مناخ مشجع للمستثمرين، وتذليل العقبات التى يواجهونها والتى تتمثل بشكل أساسى فى بطء الإجراءات وتعقيدها، مما سينعكس بشكل إيجابى على تشجيع الاستثمار المحلى وجذب المزيد من الاستثمارات الأجنبية، وتقديم الخدمات لهم وتبسيط الإجراءات الحكومية فى أقل وقت ممكن.

- رفع كفاءة أعمال الجهاز الحكومى والمراقبة والمتابعة من خلال خفض دورة الوقت المرتبطة بإنتاج وتقديم الخدمات الفورية.

- تحقيق التنسيق بين المؤسسات الحكومية مع بعضها البعض؛ حيث التشابك والاعتماد المتبادل فى المعاملات والذى يؤدى إلى التعقيدات الإدارية التى تؤدى إلى بطء الإجراءات.

(١) خالد معمر إبراهيم : أمن الحكومة الإلكترونية، الإسكندرية، الدار الجامعية، ٢٠٠٨م، ص ٦٥.

(٢) فريد النجار، مرجع سابق، ص ٢٢٦.

- تهيئة الجهاز الحكومى للاندماج فى النظام وتحقيق مستوى أداء يتواءم مع النظم الحديثة المتبعة فى الدول المتقدمة.

- توفير معلومة دقيقة محدثة لتخذ القرار وذلك للمعاونة فى التخطيط طويل المدى، المشروعات التتموية، متابعة التنفيذ بشكل دقيق.

- سهولة الوصول للخدمات إلكترونية من خلال النشر الإلكتروني وهذا يحقق مبدأ الشفافية والعدالة لكافة شرائح المجتمع وتعزيز الديمقراطية، والعمل على تحسين الخدمات من خلال التعرف على أهم معوقات الخدمات وكيفية مواجهتها وتطويرها ويحقق ذلك للمنتفعين مقدار من الثقة والثبات.

ثانياً - مشروعات وزارة الداخلية المصرية فى مجال الحكومة الإلكترونية:

قامت وزارة الداخلية بالعديد من المشروعات والتطبيقات لتنفيذ نظام الحكومة الإلكترونية متمثلة فى محورين رئيسيين وأحدهما متاح للكافة الاطلاع عليه ويتم تقديم الخدمات الجماهيرية من خلال شبكة الإنترنت؛ حيث تم إنشاء موقع خاص بوزارة الداخلية بالإضافة إلى المشاركة على بوابة الحكومة الإلكترونية وموقع خاص بمصلحة الأحوال المدنية، والمحور الثانى خاص بالماملين بوزارة الداخلية فى حدود اختصاص كل فرد يمكن مشاهدة التطبيق المسموح له بالإطلاع عليه ومن خلال شبكة معلومات خاصة بوزارة الداخلية تسمى بالإنترنت يتم تنفيذ العديد من التطبيقات الأمنية من خلالها وتحتوى على معلومات أمنية.

١- إنشاء موقع وزارة الداخلية على شبكة المعلومات الدولية (الإنترنت) :

سعت وزارة الداخلية المصرية انطلاقاً من مسئوليتها الوطنية في خدمة قضايا العمل الأمني إلى تطوير وتحديث فعاليات أداء مختلف الأجهزة الأمنية، وتم افتتاح موقع وزارة الداخلية على الشبكة الدولية للمعلومات (الإنترنت) بتاريخ ٢٤ يناير ٢٠٠٧ ليكون بمثابة التواصل بين المواطنين ووزارة الداخلية، وسوف نتناولها فيما بعد بالتفصيل المناسب.



شكل رقم (١-٤) يوضح الصفحة الرئيسية لموقع وزارة الداخلية على الإنترنت

٢- المشاركة في بوابة الحكومة الإلكترونية :

تقوم هذه الخدمة بمساعدة المواطنين الذين يرغبون في الحصول على خدمة حكومية معينة من خلال ملء الاستمارات الخاصة بهذه الخدمة والتي يمكن بسهولة تحميلها من الصفحة نفسها ومن ثم معرفة أقرب جهة يمكن للمواطن الذهاب والتقدم لها بهذا الطلب من خلال إدخال اسم الجهة مقدمة الخدمة والمحافظة ومن ثم الحي أو المدينة التي يتواجد بها المواطن وبذلك يتم إظهار أقرب جهة مقدمة للخدمة المطلوبة بكافة التفاصيل كالعنوان ورقم التليفون.

يقوم قطاع مصلحة الأحوال المدنية بمختلف الخدمات الخاصة بأوجه الحانة المدنية للمواطن المصري من حيث الميلاد والزواج والطلاق والوفاة وتسجيلها وإصدار الوثائق والمستندات الدالة عليها داخل وخارج البلاد، كما تقدم الإدارة العامة لشرطة السياحة والآثار خدمة تقديم الشكاوى للسائحين.



شكل رقم (٢-٤) يوضح الصفحة البريد الإلكتروني على شبكة الإنترنت

٣- شبكة المعلومات الداخلية لوزارة الداخلية (الإنترانت) :

تعد شبكة معلومات وزارة الداخلية (الإنترانت) هي التي تُتيح انسياب المعلومات وتبادلها بين قطاعات الوزارة بأسلوب تقني مُتطور، في إطار من السرية وعدم القدرة على اختراقها من خارج الوزارة، وقد استخدم في بناء البنية الأساسية للشبكة تقنية الإنترنت نفسها، في شكل شبكة خاصة مغلقة، تتكون البنية الأساسية لها من مجموعة من الحواسيب الكبيرة (الخادمة) التي ترتبط ببعضها عبر شبكات مغلقة، وخطوط لنقل المعلومات، وأنظمة للتأمين على مستويين العام والخاص؛ حيث تم تزويد بعض الجهات المتعاملة مع الشبكة بأجهزة حاسبات كبيرة مرتبطة مع المركز الرئيسي للشبكة لبث معلوماتها والبيانات المهمة من خلال البرامج التي تم بناؤها لتحقيق هذا الغرض، والاستفادة منها في التغلب على المعوقات الزمنية والنمطية، بما يُتيح إمكانية اتخاذ القرار السليم، بناءً على قاعدة معلومات أمنية مؤمنة، وقد تم دعم جميع جهات الوزارة بأجهزة حاسبات آلية لربطها بقاعدة البيانات المركزية، للاستفادة منها في القيام بالواجبات والمهام، وتطوير نظم العمل بقطاعات الوزارة المنوط بها تأدية خدمات جماهيرية، لتيسير وتبسيط الإجراءات على المواطنين، وهي تتكون من مركز الحاسبات بالإدارة العامة للمعلومات والتوثيق مرتبط بمجموعة من مراكز المعلومات للإدارات التخصصية، إضافة إلى شبكة معلومات استراتيجية مرتبطة بمراكز معلومات فرعية تغطي جميع القطاعات النوعية والجغرافية، والمنافذ البحرية والجوية والبرية على مستوى الجمهورية، كما ترتبط بوحدات معلومات في مراكز أقسام الشرطة، إدارات المرور، إدارات شرطة النجدة، وجميع جهات الوزارة المختلفة، وسوف نتناولها فيما بعد بالتفصيل المناسب.



شكل رقم (٣-٤) يوضح الصفحة الرئيسية لشبكة الإنترنت لوزارة الداخلية



شكل رقم (٤-٤) يوضح الصفحة البريد الإلكتروني على شبكة الإنترنت

٤ - تطبيق نظام البريد الإلكتروني :

يتطلب العمل الأمني تبادل كم هائل من المكاتبات التي كان يستخدم في تبادلها الوسائل التقليدية تماشيًا مع نظم الإدارة التقليدية التي كانت تتبع فيما قبل. ومع تطور العمل الأمني واستخدام التكنولوجيا كأحد مفردات الاستراتيجية الأمنية، مع الاعتماد على الإدارة الإلكترونية واستخدام التقنية الرقمية تم استبدال الوسائل التقليدية في تبادل المكاتبات بالوسائل الإلكترونية الرقمية وذلك باستخدام البريد الإلكتروني الآمن على شبكة الإنترنت، لتداول المكاتبات بين الجهات الأمنية المختلفة .

من خلال تحميل هذه الخدمة على شبكة المعلومات المُفَلَّقة للوزارة (الإنترنت)، والمُمتدة جغرافيًا إلى جهات الوزارة المعنية، لسرعة تبادل المراسلات في سرية تامة، واختصار الوقت، وإرسال حجم كبير من الرسائل متعددة الوسائط، وإمكانية إرسال المكاتبات لأكثر من جهة في الوقت نفسه.

وظائف ومقومات البريد الإلكتروني :

- تبادل الملفات والمعلومات والتوجيهات إلكترونياً عبر الشبكة؛ حيث يساعد ذلك في تقديم الدعم الفني للجهات المختلفة.

- إرسال رسالة بريدية إلى جهة أو جهات متعددة في اللحظة ذاتها .

- استخدام تطبيقات البريد الإلكتروني بشكل واسع على مستوى جميع جهات الوزارة وإلغاء التعامل مع البريد العادي.

- خاصية إشعار التراسل بتاريخ وساعة فتح المرسل إليه الرسالة البريدية وفي حالة إرسال رسالة بريدية إلى أكثر من جهة يقوم التطبيق بأشعار المرسل ببيان تفصيلي بالجهات التي تسلمت الرسالة والجهات التي لم تستلمها بعد وذلك من خلال التمر على موضوع الرسالة.

٥- مراكز معلومات بقطاعات الوزارة:

تم إنشاء أكثر من مائة وعشرين (١٢٠) مركز معلومات بمختلف قطاعات الوزارة، وتزويدها بأجهزة حاسبات آلية، تم ربطها بشبكة المعلومات الرئيسية، بغية بناء قواعد البيانات التي تحقق الدعم المعلوماتي للقيادات الإشرافية وأجهزة المكافحة، بما يسهم في تعزيز قدرتها على وضع خطط التأمين والضبط، واتخاذ القرار المبني على أسس علمية.

٦- شبكة التراسل الخاصة بالوزارة (Multi - Service Private Network) :

استهدفت خطة وزارة الداخلية مواكبة التقدم التطور العلمي والتكنولوجي، ارتكزت على تنفيذ الشبكة استراتيجية يمكن تحقيق الاتصال السريع من خلال شبكة خاصة مؤمنة لربط الاتصالات السلكية واللاسلكية والنقل والتبادل الفعال للبيانات والمعلومات بدرجة عالية الكفاءة بين مختلف الإدارات والمصالح في الوزارة، وتحقيق السيطرة الأمنية، ودعم وتعزيز وجود قاعدة بيانات ضخمة، يكون فيها بين مختلف الإدارات والمصالح، وهو حجر الزاوية الأساسي بما ينعكس آثاره على كفاءة الأداء، والمساعدة في اتخاذ القرار بالدقة المطلوبة وفي التوقيت المناسب، وهذه الشبكة المعروفة باسم التراسل قامت بتنفيذها الإدارة العامة للاتصالات بوزارة الداخلية، باستخدام تكنولوجيا الألياف الضوئية، من خلال وسط ترانسلي خاصة (STMI)، وتم توفيره خصيصاً لوزارة الداخلية، لربط جميع مديريات الأمن وإدارات شرطة النجدة ومحطات اللاسلكي بشبكة وزارة الداخلية، ولديها القدرة على تغطية كافة الأرجاء، وهو ما دفع الجهاز الأمني لتنفيذها وارتباطها بجميع مديريات الأمن، بالإضافة إلى كونها شبكة خاصة يضيف عنصر التأمين لتداول البيانات والمعلومات على الشبكة لصعوبة الاختراق من الخارج.

٧ - شبكة نقل المؤتمرات المرئية (Video Conference System) :

إن شبكة التراسل الاستراتيجية الخاصة بوزارة الداخلية تتيح عقد مؤتمرات مرئية مباشرة بين وزير الداخلية، مع أكثر من قيادة أمنية في وقت واحد، وذلك من خلال وحدات المؤتمرات المرئية التي تستخدمها الشبكة المنفذة، مما يساعد على تبادل الآراء ومناقشة الخطط الأمنية ومراجعتها، ويمكن أيضا من خلالها تنظيم مؤتمرات واجتماعات ولقاءات مرئية عن بُعد، لمختلف المستويات القيادية والإشرافية بالوزارة، دون حاجة للانتقال، بما يتيح سرعة تلقي البيانات والمعلومات، وترشيده اتخاذ القرار.

٨ - شبكة نقل الأحداث المرئية (Video active transmissies network) :

شبكة التراسل الاستراتيجية يمكن من خلالها نقل ومتابعة الأحداث من موقعها ولحظة حدوثها إلى جميع المستويات القيادية في الوقت نفسه، بما يمكنها من سرعة تبادل ومتابعة البيانات والمعلومات عن الحدث . واتخاذ القرار المناسب، مما يحقق الاتصال المباشر بين متخذ القرار، والقوات أثناء العمليات في أي موقع داخل مصر، مع ربط السنترالات الخاصة بوزارة الداخلية بشكلٍ موحد، وهو ما يتيح الاتصال والترابط بين مديريات الأمن وأية نقطة وموقع شرطي في المحافظات الـ ٢٧، كما يتيح هذا المشروع نقل وتبادل المعلومات واستخدام قواعد البيانات عن طريق دعم ونشر شبكات نقل المعلومات الحالية، وتفعيل مفهوم استخدامها كقاعدة بيانات وتبادلها في حدود المسموح بين هذه المصالح وبعضها البعض وبين فروعها، مما سيكون له مردود أمني واسع من حيث سرعة تلقي المعلومة، وتوفير هائل للجهد المبذول يعود على ديناميكية الحركة داخل قطاعات الوزارة وسرعة التصرف واتخاذ القرار.

٩ - مشروع الخدمة الصوتية للخدمات الأمنية الجماهيرية :

إن الخدمات الجماهيرية المباشرة كان لها اهتمامها الخاص من جانب وزارة الداخلية

ومنها خدمة الرسائل الصوتية، التي استُحدثت خصيصاً لهذا الهدف؛ حيث يقوم المواطنون بالاتصال برقم (١٢٨) من أى تليفون محمول أو عادي للدخول على الخدمة الصوتية لوزارة الداخلية للاستعلام عن الخدمات الجماهيرية التي تقدمها الوزارة للمواطنين، ومن خلالها التعرف على كافة التفاصيل والمعلومات المطلوبة للحصول على الخدمات الأمنية الجماهيرية (المرور - الأحوال المدنية - الجوازات - تصاريح العمل - الأدلة الجنائية ... إلخ)، ليتعرف المواطن على جميع المستندات المطلوبة في الإدارات والمصالح المختلفة، ونظراً للإقبال الجماهيري على هذه الخدمة؛ فقد تمت زيادة عدد الخطوط من (٢٠) خط إلى (٩٠) خط.

ثالثاً - تكنولوجيا المعلومات الأمنية في مجال تيسير وتبسيط إجراءات حصول المواطنين على الخدمات الأمنية الجماهيرية :

يميش العالم الآن عصر ثورة المعلومات، والتي ترتبط ارتباطاً وثيقاً بتكنولوجيا عصر المعلومات، وأصبحت المعرفة هي محور التقدم، وتعد الشعوب المتخلفة هي تلك التي لم تدخل ثورة المعلومات حتى اليوم، فالمعلومات هي القوة التي تحفظ للشعوب استقلالها، وتعتبر المعلومات قوة حضارية، ضرورية لتطور الشعوب وتقدمها، كما أن النمو الاقتصادي يرتبط ارتباطاً طردياً بكمية المعلومات، ونوعيتها، والطريقة التي يتم الإلمام بها، وتطبيق ما جاء فيها.

واهتمت الحكومة المصرية بتكنولوجيا المعلومات من خلال تطوير أسلوب العمل بنظام الحكومة الإلكترونية من أجل تحقيق أهداف البرنامج كان من الضروري توفير قنوات مختلفة ومتنوعة لتوصيل الخدمات إلى المواطن بالأسلوب الذي يناسبه، سواء كان ذلك من خلال الإنترنت أو التليفون أو منافذ مختلفة منتشرة على مستوى الجمهورية؛ حيث يقوم المواطن بطلب الخدمة وتقوم الهيئة القومية للبريد بتوصيلها إليه في المكان الذي

يحدده.

بوابة الحكومة المصرية^(١) :

منذ إطلاق بوابة الحكومة المصرية رسميًا عام ٢٠٠٤، يتم إتاحة العديد من الخدمات الحكومية من خلالها، وكذلك ربطها بالمواقع الإلكترونية لمختلف الجهات الحكومية والمحافظات، ويهدف البرنامج إلى إضافة خصائص جديدة للبوابة مثل إتاحة خاصية التوقيع الإلكتروني، وذلك بهدف ضمان استمرارية تشغيلها بكفاءة وفعالية، وتحقيق رضا أكبر عدد من المستخدمين من مواطنين وأجانب، وتلبية للطلب المتنامي على الخدمات الحكومية الإلكترونية.

مراكز اتصال الحكومة المصرية ١٩٤٦٨ :

يعد تقديم الخدمات الصوتية للجماهيرية من خلال مركز الاتصال ١٩٤٦٨ والذي يربط حتى الآن ما يزيد على خدمات أربعون (٤٠) جهة حكومية، بالإضافة إلى مراكز اتصال لدى الجهات التي تقدم بعض الخدمات الحكومية المستقلة مثل ١٩٩٨٤، وخدمات وزارة الداخلية من خلال الرقم (١٢٨).

منافذ تقديم الخدمات الجماهيرية :

وتوفر منافذ تقديم الخدمات الجماهيرية خدماتها للمواطنين؛ حيث يتقدم إليها المواطن بالمستندات المطلوبة، يقوم مقدم الخدمة بالتعامل مع الجهة الحكومية المختصة للحصول على الوثائق المطلوبة ثم إتمام الخدمة بتسليمها للمواطن، وهناك العديد من المواقع المرتبطة ببوابة الحكومة الإلكترونية، ويعد موقع بوابة وزارة الداخلية من أهم المواقع المرتبطة بها.

(1) www.cgyp.gov.cg

موقع وزارة الداخلية على شبكة المعلومات الدولية (الإنترنت) :

تم افتتاح موقع وزارة الداخلية على الشبكة الدولية للمعلومات (الإنترنت) بتاريخ ٢٤ يناير ٢٠٠٧م ليكون بمثابة التواصل بين المواطنين ووزارة الداخلية، وانطلاقاً من المسؤولية الوطنية في خدمة قضايا العمل الأمني وتقديم الخدمات الجماهيرية عبر موقع الوزارة، ودعمًا لعجلة التنمية والاستثمار في مختلف المجالات، وحث رجال الشرطة على الاستمرار والتطوير المستمر لما يحقق خدمة المواطنين، وتماشياً مع سياسة الدولة لتحقيق الحكومة الإلكترونية.

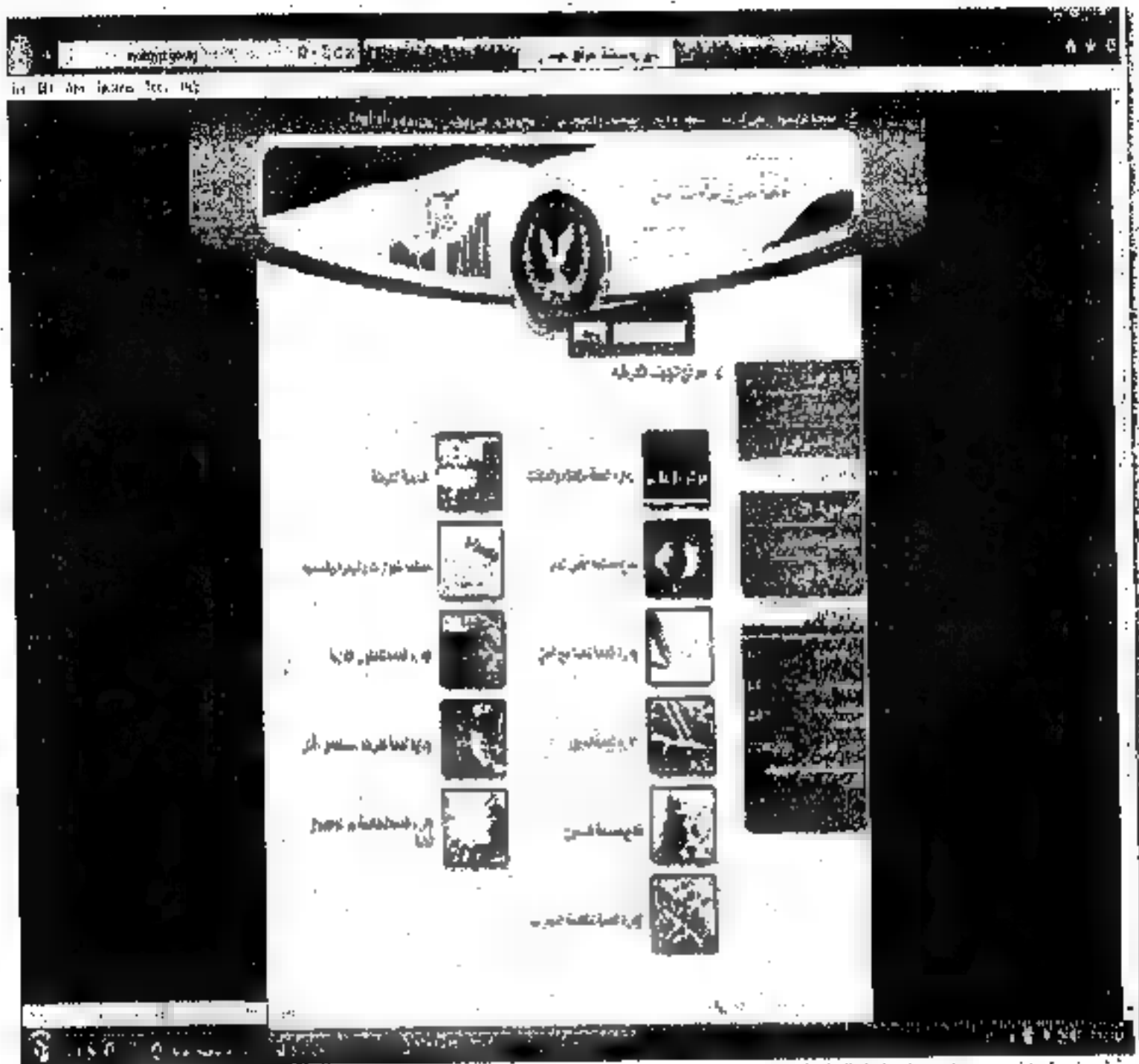
ويتضمن هذا الموقع محورين رئيسيين، وهما:

أ- المحور الإعلامي :

يتمثل المحور الإعلامي في تعريف وزارة الداخلية في المراحل التاريخية وهي أحقاب زمنية مختلفة، وكذا التعرف على الهيكل التنظيمي للوزارة بالإضافة إلى عرض الأخبار والأحداث المهمة التي تهم المواطن وإعطاء فكرة عن أنشطة القطاعات المختلفة داخل الوزارة.

ب- المحور الخدمي :

يتمثل المحور الخدمي في تقديم تلك الخدمات التي تقدمها الوزارة للمواطنين والإرشادات المرتبطة بها بالإضافة إلى بعض الأمور التي تهم المواطن وكذا البلاغات والشكاوى، وفيما يلي سوف نعرض صفحات الجهات الشرطية داخل موقع وزارة الداخلية على شبكة الإنترنت.



شكل رقم (٤-٥) يوضح مواقع الجهات الشرطية^(١)

(1) www.egypt.gov.eg

١ - الإدارة العامة للإعلام والعلاقات :

يتم من خلال الصفحة الإلكترونية للإدارة العامة للإعلام والعلاقات الإعلام عن نشاطات الوزارة والأخبار الصادرة عن المركز الإعلامي وأهم البيانات الصادرة عن الوزارة للرد على ما يثار خارجياً وداخلياً حول القضايا الأمنية في مصر وكذا المؤتمرات والندوات التي تعقدها الوزارة، بالإضافة إلى التعريف بمركز الإعلام الأمني من حيث المنشأة والأهداف وبحث البيانات الأمنية، والموجز اليومي، وعرض لأهم القضايا، ومتابعة ما تبثه وكالات الأنباء العالمية وشبكة الإنترنت وتصنيفه وأرشفته وتخزينه مع إمكانية استدعائه، وإعداد تقرير يتضمن أهم الأخبار، وبثها على شبكة معلومات الوزارة لتتاح فرصة وصول الأخبار المهمة لحظياً إلى الجميع، والاهتمام بتغطية الأنشطة التي يقوم بها السيد الوزير وتوثيقها وأرشفتها، بالإضافة لوجود رابط للاتصال بالإدارة.



شكل رقم (٦-٤) يوضح موقع الإدارة العامة للإعلام والعلاقات

٢- أكاديمية الشرطة :

تحتوي هذه الصفحة على عرضاً كاملاً عن أكاديمية الشرطة وأهدافها والكليات التابعة لها وأهم الأنشطة وشروط الالتحاق وخطة الدراسة بكلية الشرطة، كما يتم بث آخر أبحاث مركز بحوث الشرطة والندوات والمؤتمرات التي ينظمها، كما يتيح تلك الصفحة الدخول على تطبيق التقديم كلية الشرطة ويتم من خلاله تسجيل بيانات الطلبة المتقدمين للاختبارات، وعرض نتائج كافة الاختبارات للطلبة المتقدمين من خلال شبكة معلومات الوزارة.



شكل رقم (٧-٤) يوضح موقع أكاديمية الشرطة

٣ - قطاع مصلحة الأمن العام :

تعرض صفحة مصلحة الأمن العام موجز عن الإلتربول وتعريف عن إدارة الشرطة الجنائية الدولية العربية (إنتربول القاهرة) ودورها في مجال مكافحة الجريمة، وفي إطار اهتمام وزارة الداخلية بمجالات الغياب والبحث المجهولة والضالين وفاقدي الذاكرة والمصابين والمرضى المجهولين، تضمنت صفحة مصلحة الأمن العام عرض للمفاتيح لإتاحة الفرصة لمستخدمي شبكة الإنترنت الاطلاع على البيانات والمعلومات والصور الخاصة بتلك الحالات للمساهمة في الاستدلال عليهم، والاهتداء لأسرهم من خلال إتباع الإجراءات الموضحة بالموقع.



شكل رقم (٨-٤) يوضح موقع قطاع مصلحة الأمن العام

٤ - مصلحة الجوازات والهجرة والجنسية:

تتضمن صفحة مصلحة الجوازات والهجرة والجنسية، عرض وتصنيف الإجراءات المتعلقة بإصدار وثائق السفر، ومنح تصاريح الإقامة، وحركة المسافرين والداخلين عبر المنافذ الشرعية للبلاد، والإجراءات الخاصة بالهجرة والجنسية، وإقامة الأجانب، وكافة الخدمات التي تقدمها المصلحة من وثائق السفر وطلبات الهجرة والجنسية وشهادات التحركات وتنفيذ الأحكام القضائية بالإضافة إلى قواعد سفر المواطنين للخارج، بهدف تطوير وتبسيط إجراءات الجنسية، والهجرة، والإقامة، وإجراءات إصدار وثائق السفر، ودقة وسرعة الحصول على البيانات المتعلقة بحركة السفر والوصول للمواطنين والأجانب، كما تضمنت الصفحة نبذة تاريخية عن المصلحة، والإجراءات المطلوبة لإصدار وثائق السفر، وقواعد سفر المواطنين للخارج، ونموذج طلب الشهادات للجهات القضائية، وطلبات تنفيذ الأوامر الوقتية والأحكام القضائية، وقسم البلاغات، وتعريف بأقسام الجوازات والمنافذ البرية والبحرية والجوية على مستوى الجمهورية.



شكل رقم (٤-٩) يوضح موقع مصلحة الجوازات والهجرة والجنسية

٥- الإدارة العامة لتصاريح العمل :

تضمن هذه الصفحة دور الإدارة في المجالات المختلفة الأمنية والاقتصادية والخدمات الجماهيرية التي تقدمها، وشروط وإجراءات حصول المواطن عليها وتيسير استخراج تصريح العمل، كما تضمن نموذجاً يمكن للمواطنين الراغبين في تجديد تصريح العمل الخاصة بهم، ويهدف إصدار تصريح العمل وفقاً للقواعد، وتبسيط إجراءات إصدارها وتجديدها، ويتم التعامل مع هذا النموذج وإرسال البيانات المطلوبة ودفع الرسوم إلكترونياً عبر الإنترنت للإدارة العامة لتصاريح العمل لتجديد التصريح المطلوب، ويخدم ذلك عددًا كبيراً من العاملين في الخارج وييسر تقديم الخدمة لهم.

شكل رقم (١٠-٤) يوضح موقع الإدارة العامة لتصاريح العمل

٦- الإدارة العامة للشئون الإدارية :

تتضمن الصفحة الإلكترونية للإدارة العامة للشئون الإدارية خدمات الإدارة في مجال الحج والعمرة، المتعلقة بشروط وقواعد وإجراءات الحج والعمرة، لتبسيط وتيسير إجراءات المواطنين للحج والعمرة، ودقة المعلومات والبيانات، ومتابعة إجراءات السفر للحج والعمرة طبقاً للقواعد المقررة، والإرشادات العامة للحجاج المصريين تعد من الأمور المهمة التي تحرص عليها الوزارة، والعمل على خلق الارتباط والتواصل بين الوطن وحجاج بيت الله الحرام بالأراضي السعودية في مواسم الحج، وبث الأخبار المهمة والتيسيرات التي تقدمها في هذا المجال، وأيضاً التصديق على الشهادات وتعرض لضوابط تعيين العمدة والمشايخ.



شكل رقم (١١-٤) يوضح موقع الإدارة العامة للشئون الإدارية

٧- الإدارة العامة للمرور :

تعرض هذه الصفحة أهم الأتيار المرتبطة بالمرور والتي تهه المواطن بالإضافة إلى قواعد وأداب المرور والجديد في هذا المجال وخدمات المرور والعقوبات المرتبطة به عن طريق ميكنة جميع البيانات الخاصة بالمركبات ورخص القيادة والحوادث والمخالفات المرورية، بنية تبسيط الإجراءات الخاصة باستخراج رخص القيادة ورخص تسير المركبات، وشهادة البيانات، وتلبية الاحتياجات الأمنية من معلومات عن المركبات ورخص القيادة بدقة فائقة، وإصدار تراخيص ميكنة وغير قابلة للتزوير.



شكل رقم (١٢-٤) يوضح موقع الإدارة العامة للمرور

٨- الإدارة العامة لشرطة السياحة والآثار :

تعد هذه الصفحة لتلقي البلاغات و الشكاوى من السائحين من الأمور المهمة لمواجهة أية صور استغلال أو لدراسة المصاعب التي تواجه السائحين في مجالات التعامل اليدوي، مما يعد مصدراً مهماً لمواجهة صور الإساءة أو الاستغلال المختلفة أو لتصحيح الأمور التي تُشكل مصاعب أو مشاكل للسائحين وذلك بهدف الوصول إلى أفضل مستوى من الخدمة الأمنية لزائري جمهورية مصر العربية من الاطمئنان والراحة ودعمًا للتنمية والاستثمار في مجال السياحة.



شكل رقم (١٣-٤) يوضح موقع الإدارة العامة لشرطة السياحة والآثار

٩- قطاع مصلحة السجون :

دعماً لحقوق الإنسان فإن صفحة مصلحة السجون تتعرض لأهم أوجه الرعاية الاجتماعية والصحية للسجناء بالإضافة إلى نبذة عن قطاع مصلحة السجون وتطور السياسة العقابية في السجون المصرية وتأهيل السجناء وتوفير فرص العمل لهم، كما تتضمن الصفحة تعريفاً للخدمات الجماهيرية التي تقدمها المصلحة للمواطنين القادمين لزيارة ذويهم سواء كانت الزيارة عادية أو خاصة وكيفية صرف المساعدة المالية أو المعاش لأسر المسجونين.



شكل رقم (١٤-٤) يوضح موقع قطاع مصلحة السجون

١٠ - الإدارة العامة لمكافحة المخدرات :

تهدف هذه الصفحة إلى نشر الوعي لدى الجمهور إلى الآثار الضارة للمخدرات ونشر تعريف عن الإدارة العامة لمكافحة المخدرات، والأجهزة الوطنية للمكافحة، وعرض للتقرير السنوي، والتدريب في مجال المكافحة، والتطور التشريعي في هذا المجال، وعرض لأهم أنواع المخدرات، والآثار الضارة للمخدرات، وتناول طرق التوعية، وأهم القضايا والآثار الاجتماعية والصحية والاقتصادية الأمنية وعرض لمكتب الإدارة، ومتحف الإدارة، وفي النهاية البلاغات، مما يساهم في زيادة الوعي لأخطار المخدرات.



شكل رقم (١٥-٤) يوضح موقع الإدارة العامة لمكافحة المخدرات

١١ - الإدارة العامة لمكافحة جرائم الأموال العامة :

تهتم صفحة الأموال العامة بتثقيف الوعي لدى الجمهور في مجال الجرائم المرتبطة بالأموال العامة من خلال نشر العلامات ووسائل التأمين الخاصة بالعملات الوطنية والأجنبية، وأهم الإرشادات في التفرقة بين العملات الوطنية والأجنبية الصحيحة والمقلدة، ومعلومات عن مخاطر الهجرة غير المشروعة، وعن خطورة ظاهرة الرشوة وتأثيراتها السلبية على الوظيفة العامة، مع عرض جانب من الجرائم التي تم ضبطها، وبعض التوجيهات لتجنب الوقوع ضحية للنصب والاحتيال وجرائم غسل الأموال وسفر العملة المصرية للخارج، ليكون لدى المواطن دراية بهذه الأمور وتجنب الوقوع ضحية لمثل هذه الجرائم وإرسال البلاغات عبر الشبكة للإدارة العامة للأموال العامة لزيادة التفاعل بين المواطن والوزارة في مكافحة هذه الجرائم.



شكل رقم (١٦-٤) يوضح موقع الإدارة العامة لمكافحة جرائم الأموال العامة

١٢ - قطاع مصلحة الأحوال المدنية

في إطار سياسة وزارة الداخلية لتقديم كافة التيسيرات للمواطنين للحصول على الخدمات باستخدام تكنولوجيا المعلومات والاتصالات فقد تم تطوير أسلوب تقديم عدد من خدمات قطاع مصلحة الأحوال المدنية متمثلة في (شهادات الميلاد المميكنة - بطاقات الرقم القومي «بدل فاقد/تالف») لمن سبق لهم استخراج بطاقة الرقم القومي ليتمكن المواطن من الحصول على الوثائق المطلوبة عن طريق البريد السريع باستخدام شبكة المعلومات الدولية على الموقع التالي (www.cso.gov.eg)، ودون حاجة للانتقال إلى مقر المصلحة؛ حيث يقوم المواطن بالدخول على موقع قطاع مصلحة الأحوال المدنية أو الدخول من خلال بوابة الحكومة الإلكترونية واختيار خدمات مصلحة الأحوال المدنية، أو الدخول على موقع وزارة الداخلية واختيار خدمات مصلحة الأحوال المدنية، وملء البيانات الخاصة بالمستند المطلوب ثم سداد قيمة المستندات وتكلفة البريد من خلال بطاقات الائتمان (فيزا، ماستر كارد) يتولى قطاع مصلحة الأحوال المدنية مراجعة البيانات وإصدار الوثائق على أن يتولى البريد السريع توصيل الخدمة للمنازل خلال ٤٨ إلى ٧٢ ساعة، وأيضاً يمكن الاستعلام عن موقف الخدمة في غضون أسبوع من طلبها في حالة تأخرها لاحتمال وجود اختلاف في البيانات المطلوبة عن المسجلة على الحاسب يجب على المواطن التوجه إلى المصلحة أو الإدارات التابعة لها بالمستندات الدالة على البيانات المطلوبة لتصحيحها بالسجلات.

هذا ويحق لقطاع مصلحة الأحوال المدنية رفض تقديم تلك الخدمة عن طريق الإنترنت لغير المستفيدين السابق إيضاحهم ويمكن لطالب الخدمة التوجه إلى أحد أفرع المصلحة للاستفسار.

وفيما يلي قائمة بالخدمات التي تقدمها مصلحة الأحوال المدنية مقسمة طبقاً لنوعياتهم:

وقائع الميلاد :

استخراج شهادة الميلاد أول مرة، استخراج صورة قيد شهادة ميلاد لأول مرة ممكنة، استخراج صورة قيد شهادة ميلاد للتوصلات بالخارج، فحص طلب قيد ساقط الميلاد إذا تقدم بالطلب قبل مرور عام من تاريخ الميلاد، فحص طلب قيد ساقط الميلاد إذا تقدم بالطلب بعد مرور عام من تاريخ الميلاد.

وقائع الزواج والطلاق :

استخراج صورة قيد الزواج الممكنة، استخراج صورة قيد الطلاق الممكنة، وقائع الوفاة، استخراج شهادة الوفاة أول مرة، استخراج صورة قيد شهادة وفاة ممكنة، فحص طلب قيد ساقط الوفاة إذا تقدم بالطلب قبل مرور عام من تاريخ الوفاة، فحص طلب قيد ساقط الوفاة إذا تقدم بالطلب بعد مرور عام من تاريخ الوفاة.

إصدار بطاقة الرقم القومي والقيد العائلي الممكن :

إصدار بطاقة الرقم القومي (أول مرة، بدل فاقد، بدل تالف، تغيير بيانات، إعادة تصوير) مستخرج القيد العائلي الممكن تغيير، تصحيح قيود الأحوال المدنية تغيير قيود الأحوال المدنية المدونة بالسجلات تصحيح قيود الأحوال المدنية المدونة بالسجلات.

الخدمة	الرسوم
الخدمات العامة	10.000
الخدمات الخاصة	10.000
الخدمات التجارية	10.000
الخدمات المالية	10.000
الخدمات الصحية	10.000
الخدمات التعليمية	10.000
الخدمات الثقافية	10.000
الخدمات الرياضية	10.000
الخدمات الترفيهية	10.000
الخدمات الاجتماعية	10.000
الخدمات البيئية	10.000
الخدمات الأمنية	10.000
الخدمات الدفاعية	10.000
الخدمات الخارجية	10.000
الخدمات الداخلية	10.000
الخدمات العامة	10.000
الخدمات الخاصة	10.000
الخدمات التجارية	10.000
الخدمات المالية	10.000
الخدمات الصحية	10.000
الخدمات التعليمية	10.000
الخدمات الثقافية	10.000
الخدمات الرياضية	10.000
الخدمات الترفيهية	10.000
الخدمات الاجتماعية	10.000
الخدمات البيئية	10.000
الخدمات الأمنية	10.000
الخدمات الدفاعية	10.000
الخدمات الخارجية	10.000
الخدمات الداخلية	10.000

شكل رقم (١٧-٤) يوضح موقع قطاع مصلحة الأحوال المدنية

١٣ - مصلحة الأدلة الجنائية

من خلال حصر وتصنيف وتبويب وميكنة البيانات المتعلقة بإجراءات إصدار مصحف الحالة الجنائية، بغية تبسيط وتيسير إجراءات إصدار مصحف الحالة الجنائية وعدم تزويرها، وقد تم استحداث صحيفة الحالة الجنائية المتكررة (بدون بصمات)؛ حيث يمكن للأشخاص حاملي بطاقات الرقم القومي استخراج هذه الصحيفة بدون أخذ البصمات مرة أخرى، في حالة أخذها مسبقاً، وأيضاً المستندات والأوراق اللازمة للحصول على خدمة إصدار نموذج صحيفة الحالة الجنائية، والتصديق على صحيفة الحالة الجنائية.

الفصل الخامس

دور التقنيات الحديثة في تطوير
تكنولوجيا المعلومات الأمنية

الفصل الخامس

دور التقنيات الحديثة في تطوير تكنولوجيا المعلومات الأمنية

إن التطور التكنولوجي والتقني الذي يعيشه العالم الآن، جعل التحقق من هوية الأشخاص أمرًا يزداد صعوبة، وقد استلزم هذا التطور الذي يشهده العصر واستفادات منه العناصر الإجرامية في ارتكاب الجرائم، إلى تطوير وتحديث الإجراءات الأمنية، وبعد استخدام البصمات البيومترية في التحقق من هوية الأشخاص من خلال صفاته الفسيولوجية أو سماته السلوكية التي يمكن التعرف عليها والتأكد منها آليًا، إحدى الوسائل التي تعتمد عليها الأجهزة الأمنية في كشف الجرائم ومركبها.

وفي ضوء ما تقدم، سنتناول هذا الموضوع على النحو الآتي :

أولاً، مفهوم التقنية البيومترية .

ثانيًا، بصمة الإصبع .

ثالثًا، البصمة الوراثية .

أولاً - مفهوم التقنية البيومترية :

انتشرت التقنية البيومترية بشكل ملموس وسريع في الفترة الماضية، وهي تعد القاعدة الأساسية للتعرف الآمن على الهوية، وتشكل الجزء الأساسي من الأنظمة التي تتطلب تحديدًا دقيقًا للهوية، وكثرت تطبيقاتها في المطارات بشكل خاص، وحولت الكثير من الدول جوازات سفرها وتأشيرات دخولها إلى الشكل البيومتري ليس فقط للمزايا الأمنية التي تتمتع بها، بل أيضًا لما تتمتع به من الملائمة والسهولة في الاستخدام، كذلك كثر استخدام تقنياتها المختلفة للمراقبة، أو كأساس لأنظمة التحكم في دخول أماكن محددة، إلا أن تلك التطبيقات الآن أصبحت منتشرة بشكل كبير حتى وصلت إلى جهاز الكمبيوتر الشخصي لتستخدم كوسيلة لحماية المعلومات.

أصل كلمة «بيومتري» يرجع إلى اللغة اليونانية وينقسم اللفظ إلى جزأين «بيو» وتعني الحياة، و«مترية» تعني لأجل القياس، فالتكنولوجيا البيومترية تعتمد على المميزات الخاصة في الجسم، وهي عبارة عن علم يدرس كيفية استخدام معادلات رياضية وإحصائية لقياس العلاقات الرقمية والنسب المختلفة التي تظهر في الكائنات الحية وأعضائها المختلفة، وتسمح بتصوير مصادقات الطبيعة بشكل حسابي وذلك باستغلال كل من نظريات علم الرياضيات وعلم الإحصاء، ويتم التعرف على تلك الصفات عبر جهاز الكمبيوتر الذي يتعرف على بصمات الإصبع عبر المجسات المختلفة مثل الماسح الضوئي لبصمات الأصابع أو ماسح العين والوجه أو قارئ الخطوط الإلكترونية عبر معادلات رياضية دقيقة ومعقدة، يقارن جهاز الكمبيوتر تلك المعلومات بما هو مخزن لديه ليحدد إذا كانت تتطابق معها أم لا (1).

(1) L.C. Jain : Intelligent Biometric Techniques in Fingerprint and Face Recognition, Boca Raton: CRC Press, C1999, p21

وأشكال التقنيات البيومترية كثيرة ومتنوعة، فمنها تقنية التعرف على الوجه أو العينين أو شكل الأذنين إلى التوقيع اليدوي أو طريقة الكتابة على لوحة المفاتيح مروراً ببصمات الأصابع والشكل الهندسي للميز لليد والحمض النووي المعروف باسم (دي. إن. إيه (DNA) والتعرف على بصمة الصوت والرائحة المميزة لكل جسد وغيرها من الوسائل المتعددة والمميزة لكل فرد، إلا أن الكثير من تلك التقنيات يعد باهظ الثمن بشكل كبير، ولا يستطيع الكثيرون الاعتماد عليه، لذلك فقد أصبحت تقنية التعرف على بصمة الأصابع الأكثر انتشاراً لأنها الأقل تكلفة، وتتبع بصمة مكانة متميزة بين المحددات البيومترية المتنوعة نظراً لما تتمتع به من مزايا، وقد تم اعتمادها للتعرف على الهوية، وتأمين الدخول والخروج من وإلى المؤسسات، يتكون هذا النظام بشكل أساسي من وحدة معالجة إشارة تقوم باستخلاص السمات المميزة للبصمة والتعرف عليها، ومن حاسب شخصي لإدارة النظام، ومن البرمجيات الخاصة بالتطبيق المذكور للنظام.

لمحة حول الأنظمة البيومترية :

البيومترية تعني الطرق المؤتمنة للتعرف على الهوية والمعتمدة على المواصفات الفيزيولوجية والسلوكية للشخص المعنى، وتشمل المواصفات الفيزيولوجية أنواعاً عديدة من المحددات مثل البصمة، مقاييس اليد، التعرف على قرحة العين، التعرف على شبكة العين، التعرف على الوجه، كما تشمل المواصفات السلوكية أنواعاً عديدة من المحددات -أيضاً- مثل الصوت، التوقيع، النقر على الملامس (عند الطباعة)، طريقة المشي، التعرف على خط اليد.

تجدر الإشارة إلى أن استخدام الأنظمة البيومترية للتعرف على الهوية ملائم بشكل ملموس؛ (حيث لا يوجد ما يلزم حمله أو تذكره مثل كلمات المرور أو الأرقام أو البطاقات

الشخصية) ، وأصبحت هذه الأنظمة مقبولة اجتماعيًا وغير مرتفعة التكلفة.

وانتشار هذه الأنظمة في نمو مستمر ليس فقط للمزايا الأمنية التي تتمتع بها، إنما أيضًا لما تتمتع بها من الملائمة والسهولة في الاستخدام، وتتكون الأنظمة البيومترية من جزئين هما الكيان الصلب، وهو متمثل في الأجهزة والأدوات، والكيان اللين، وهو متمثل في البرمجيات.

وتشكل عملية التقاط مواصفات المحدد البيومتري مرحلة التسجيل في النظام البيومتري؛ حيث يتم فيها إدخال البيانات إلى النظام بواسطة الأداة المناسبة (ماسح، كاميرا، ميكروفون ... إلخ)، ثم تقوم برمجيات النظام باستخلاص السمات المناسبة من الشكل الذي تم إدخاله، وتخزين البيانات العائدة له على شكل «قالب»، وعندما يتعامل المستخدم مع النظام البيومتري ثانية فإن النظام يقوم بمقارنة بيانات المستخدم المدخلة مع القالب المخزن مسبقًا عنه، فإن حصل التطابق تم التعرف، وإلا فلا تسمح له، ويمكن إعطاء الحق لأكثر من شخص للدخول إلى النظام، فالكومبيوتر الشخصى يمكن إعطاء الحق لأكثر من شخص بالدخول عليه، وكذلك لبوابة المنزل أو غيرها، قد لا تحتاج للمفاتيح أو البطاقات فيما بعد فإصبعك يكفى للتزويد بتلك المعلومات أو نقلها، والشركات يمكنها تخزين معلومات تخص مئات الأشخاص، ولا تفتح الأبواب إلا إذا تطابقت البصمات المسوح لها مع تلك المعلومات المخزنة.

استخدام البصمات البيومترية في التحقق من هوية الأشخاص :

إن التطور التكنولوجى والتقنى الذى يمشه العالم الآن جعل التحقق من هوية الأشخاص أمرًا يزداد صعوبة، ويرجع ذلك إلى تراجع الاتصال المباشر بين الأشخاص فى حياتهم اليومية بسبب الأجهزة والتقنيات التكنولوجية الحديثة فأغلب التعاملات تتم من خلال عمليات بسيطة على شبكة الإنترنت.

وقد استلزم هذا التطور الذي يشهده العصر واستقادت منه العناصر الإجرامية في ارتكاب الجرائم، أهمية تطوير وتحديث الإجراءات الأمنية، ويعد استخدام البصمات البيومترية في التحقق من هوية الأشخاص، إحدى الوسائل التي تعتمد عليها الأجهزة الأمنية في كشف الجرائم ومركبيها.

أهم الوسائل البيومترية لتحقيق الهوية :

١ - بصمة الأصابع :

تكسو أصابع يد الإنسان خطوط طمية بارزة توازيها أخرى غائرة، وتأخذ هذه الخطوط مسارات متعددة الاتجاهات، لتكون مجموعة من الأشكال الرئيسية والفرعية تتباين فيها العلامات المميزة لدرجة يصعب معها حصرها، وتبدأ تكوين هذه الأشكال بأطراف الجنين؛ حيث تكتمل سماتها المميزة في الشهر السادس من الحمل، وتظل هذه الأشكال ثابتة لا يمتريها التغيير إلى ما بعد الوفاة، فهي آخر خلايا النسيج البشري في التحلل عدا ما يمكن أن يطرأ عليها من اتساع أو نعومة أو آثار لالتحام الجروح أو الحروق.

تتمثل وظيفة نظم التوثيق من خلال بصمات الأصابع التحقق من تطابق البصمات الرقمية للشخص المفحوص مع البصمات الرقمية التي تم تسجيلها مسبقاً للشخص نفسه فعند تسجيل البصمة يتم دعوة المستخدم لوضع إصبعه على جهاز القارئ، ثم يتم تحويل الصورة إلى بصمة رقمية يتم تحليلها للحصول على العلامات المميزة للبصمة، ثم يتم تخزينها على أقراص أو بملفات، أما عند التحقق من هوية شخص يتم دعوته إلى وضع إصبعه على جهاز القارئ، ثم تحول الصورة إلى صورة رقمية وتحلل لمعرفة العلامات المميزة، ثم تتم مقارنة البصمة المحولة مع البصمات التي سبق تسجيلها

للشخص نفسه، ومن خلال ذلك يسمح النظام ويرفض دخول الشخص وفقاً لنتيجة تطابق بصمته مع البصمة التي سبق تسجيلها للشخص نفسه⁽¹⁾.

٢ - بصمة حدقة العين :

«الحدقة» هي الجزء الدائري الملون من العين، وهو الذي يتحكم في نسبة الضوء التي تدخل العين عن طريق فتح الحدقة وضمها بواسطة عضلة قابضة تتحكم في حجم حدقة العين فتسمح لمزيد من الضوء بالدخول للعين عندما يكون المكان مظلماً وتسمح لكمية أقل من الضوء عندما يكون المكان مضاءً.

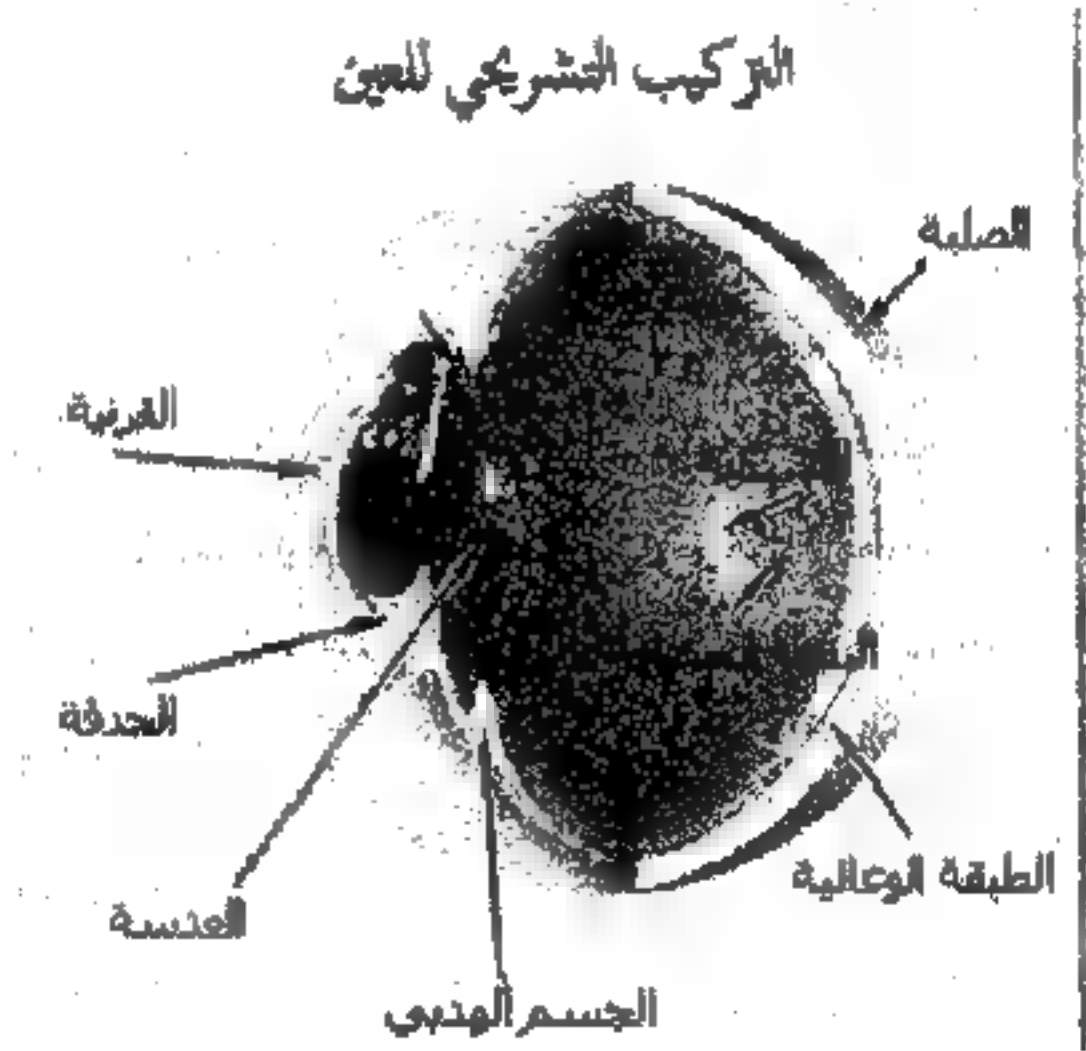
وتستخدم في التصوير كاميرا متخصصة يقف أمامها الشخص، وترسم هذه الكاميرا خريطة واضحة للحدقة بدايةً من الحروف الخارجية للحدقة، ثم تنتقل تدريجياً إلى المميزات الداخلية، وتسجيل البصمة لأول مرة يستغرق دقائق محدودة، والنظارات والعدسات اللاصقة لا تؤثر على المسح، ولا يتطلب توسع العين من جفونها لالتقاط الصورة أو التصاق مباشر بالكاميرا، أو تسليط ضوء في قاع العين كما هو حال بصمة شبكية العين، إلا أن تصوير الشخص بعدسة ذات حدقة مصطنعة يؤدي إلى خلل بالنظام.

تحتوي حدقة العين على كم من المعلومات جعلها أكثر عضو مميز في جسم الإنسان على الإطلاق وجعل «البصمة الحدقية» أكثر تفوقاً في دقتها على كل الأنواع الأخرى ومن أجل التعرف على شخص، فالمسح الحدقي يتميز عن غيره من الوسائل بعدم وجود حدقتين متشابهتين في حدق البشر حتى في التوائم المتماثلة، بل إن الحدقة اليمنى ذاتها مختلفة عن اليسرى في الشخص الواحد، بالإضافة إلى أن رسم الحدقة ثابت

(1) Nalini Ratha, Ruid Bolle : Automatic Fingerprint Recognition Systems, New York: Springer, c2004, P52.

طوال العمر؛ حيث يتكون رسمه بعد ستة أشهر من الولادة ويثبت بعد سنة من العمر ويستمر في ثباته حتى الوفاة إلا في بعض العمليات الجراحية أو الحوادث النادرة، وعلى الشخص وقتها أن يعيد تسجيل بياناته حديثة.

المسح الحيقي هو الأكثر دقة وبساطة وخصوصية فيستحيل فيه أي نوع من التقليد، وأية مؤسسة تتعامل باستخدام المفاتيح، الكروت بأنواعها، الوثائق، الكلمات والأرقام السرية يمكن أن تستخدم هذا النوع من التكنولوجيا^(١).



شكل رقم (١-٥) يوضح التركيب التشريحي للعين

(١) حسين الحمدي بواذي: الوعائل الطبية الحديثة في الإثبات الجنائي، الإصدار الثاني، ٢٠١٥م، ص ٦٤.

٣- بصمة راحة اليد :

إن استخدام الشكل الهندسي لليد هو الوسيلة الأكثر انتشاراً واستخداماً للتحكم في المنافذ ويقوم النظام بالتحقق من (٩٠) علامة بما فيها البعد الثلاثي لليد وطول وعرض الأصابع وشكل المفاصل، والتقاط صورة لليد والحصول على معلومات عنها تستخدم الأشعة تحت الحمراء وكاميرا رقمية؛ حيث يضع المستخدم يده على لوح به علامات إرشادية لوضع الأصابع وتعطى أجهزة قراءة هندسة اليد مستوى عال جداً من الدقة إلا أنها يمكن أن تحظى فيها بين التوائم أو أفراد العائلة الآخرين، كما أن هذه الأجهزة ذات حجم كبير مما يعوق استخدامها في بعض التطبيقات.

٤- بصمة سمات الوجه :

يتم استخدام قياسات خاصة بتباعد العينين وحجم الأنف وعرض الفم للتعرف على هوية الأشخاص، وتستخدم معظم نظم التحقق من الوجه وسيلة نموذجية وهي جهاز الكمبيوتر وكاميرا لالتقاط الصورة وتسجيلها في قاعدة معلومات، وتستخدم تلك النظم قياسات تباعد بين مختلف أجزاء الوجه كوسيلة للتحقق من الشخص، إلا أن وجود متغيرات مثل النظارات الشمسية والنقن وتعبيرات الوجه غير العادية وانحناء الرأس يمكن أن تسبب خللاً بنظام تحديد الوجه^(١).

٥- بصمة الصوت :

لكل صوت آياً كان مصدره مميزات وخواص معينة عن طريقها يمكن تمييزه عن مختلف الأصوات، وتتلخص هذه الخواص فيما يلي:

الدرجة : هي خاصية الصوت التي تجعلنا نميز بين نغمة غليظة ونغمة رفيقة.

(1) L.C. Jain : Intelligent Biometric Techniques in Fingerprint and Face Recognition, op.cit. p463

الشدة، هي خاصية الصوت التي تجعلنا نميز بين نغمة قوية ونغمة ضعيفة.
النوع، وهي خاصية الصوت التي تجعلنا نميز بين نوع المصدر الذي يصدر هذا الصوت أو هذه النغمة ويميز بين صوت بسيط، وأصوات معقدة أو مركبة.
 ويعتبر تحديد الصوت هو أحد الأشكال العادية جداً في التكنولوجيا البيومترية لأنها لا تتطلب أى اتصال جسدى مع الجهاز القارئ بالنظام وتعتمد نظم تحديد الصوت على صفات الصوت الفريدة لكل شخص، وتستخدم أغلب نظم تحديد الصوت عرض نص ما وكلمات خاصة على الشخص قراءتها ونطقها من أجل التحقق من أن الشخص الجارى التحقق من هويته موجود ولا يتعلق الأمر بتسجيل له.

٦- بصمة شبكة العين :

هي الطبقة الحسية للعين ويخل فيها عدد كبير من الشعيرات الدموية التي يمكن أن يتغير شكلها من السن والمرض ولا يتغير شكلها الهندسى، فهي بصمة مميزة لكل شخص يمكن قياسها من خلال حزمة ضوئية يتم تسليطها على عين الشخص المراد التعرف عليه وتتميز تلك التقنية بأنها من أكثر الوسائل التي يمكن الوثوق بها في تحديد هوية التوائم المتماثلين ولكنها مكلفة للغاية.

وتلتقط الأجهزة القارئة حتى ١٩٢ نقطة أو علامة مميزة، يمكن استخدام هذا النوع من تحديد الهوية في تطبيقات أمان عالية للغاية.

٧- بصمة التوقيع :

إن التحقق (الحركى) من التوقيع يقوم على التفرقة بين أجزاء التوقيع المعتادة. وأجزاء التوقيع التي تختلف مع كل توقيع، وتحتوى نظم التحقيق من الهوية من خلال التوقيع والمسح باستخدام قلم قارئ، ويتم التحقق من تحليل بعض المتغيرات منها سرعة التوقيع وزيادة سرعة التوقيع والضغط ... إلخ، ويتم ربط لوحة كتابة حساسة بجهاز

حاسب إلى يتم الكتابة عليه بقلم إلكتروني وفارة ويستخدم النظام برنامجًا خاصًا يعمل بالارتباط بقلم إلكتروني ويتم وفقًا لهذا النظام تسجيل حركات مستخدم القلم منها سرعة الكتابة، وتغيرات القلم وحساب المسافة ما بين الأحرف من خلال أخذ ثلاث عينات من التوقيعات يتم تحليلها وتسجيل التحليلات الناتجة في قاعدة بيانات ويتم مضاهاة التوقيعات لمعرفة هوية الشخص⁽¹⁾.

ثانيًا - بصمة الإصبع:

البصمة هي حافة أصابع الأيدي، وأصابع القدمين، وكذلك راحة اليد، وراحة القدم، تحمل أثرًا طبيعيًا، عبارة عن صف من المسامات، متشكلة على شكل خرائط مناسبة (Contour Map) ذات خطوط مناسبة أو كفاف (الشكل المنحرف أو المتعرج)، هذه الخطوط والمسامات تفرز عرقًا، والعرق يترك شكل مسامات على الأجسام الأخرى، خصوصًا اللصاق، عند ملامستها لها، وهو ما يسمى «طبعة البصمة»، وتمتاز البصمات بخاصية تُعرف بالتفرد أو الفردية، إذ أن كل إنسان يحمل طبعة بصمة خاصة به، لم يثبت إلى الآن، تماثلها مع طبعة أو بصمة غيره.

وللبصمة صفات مميزة لكل شخص، فهي تتشكل عند الجنين حتى الأشهر السبعة الأولى من تكوينه، وتبقى مع الإنسان طيلة حياته، مع الإشارة إلى أن استخدام البصمة للتعرف على الهوية يعود إلى منتصف القرن التاسع عشر الميلادي، وشهد استخدامها تطورًا مهمًا في نهاية القرن المذكور، كما أصبح استعمالها للتعرف على الهوية معتمدًا من الجهات القانونية، ويعود ذلك للمكانة المميزة التي تتبوؤها البصمة بين المحددات البيومترية المتنوعة المستخدمة للتأكد من الهوية⁽²⁾.

(1) Nalini Ratha, Ruud Bolle, op.cit, p45.

(2) Henry C. Lee, R.B. Gaensslen : Advances in Fingerprint Technology, 2nd ed, Boca Raton, Fla. : CRC Press, c2001, p 43.

لذلك فقد سعى العلماء لاكتشاف وسائل تجعل الكشف عن البصمات أكثر أماناً، الطريقة البصرية المنتشرة بشكل كبير تعتمد على صورة البصمة، فهي تقارن الشكل فقط، وهو ما دفع البعض للاتجاه إلى قياس مقاومة الجلد بالإضافة إلى الشكل، والطريقة الأكثر أماناً هي الطريقة الحرارية؛ حيث تعتمد على قياس فرق درجة الحرارة بين المرتفعات والمنخفضات في الإصبع أثناء ضغطه على الجهاز، وتعد هذه هي بصمة الإصبع التي تتم مقارنتها بالمعلومات المخزنة بقاعدة البيانات في تلك التقنية الجديدة، هذه المعلومات الدقيقة تميز اليد، كما أن الإصبع يحمل في المتوسط ٣٠ علامة دقيقة مميزة من سبعة أنواع مختلفة، وطريقة التخزين أيضاً مهمة جداً، ولذلك فتعتمد اعتماداً كبيراً على العلامات الدقيقة في الإصبع ونخزنها عن طريق الأعداد الثنائية (٠، ١)، ومن غير الممكن حساب بصمة الإصبع عبر هذه الشفرة، ولكن بالتأكيد استخدام أكثر من ميزة بيومترية والجمع بينها هو ما يمكن أن يعطى أكبر قدر من الأمان لفتح الأبواب أو التعامل مع المعلومات.

واليوم يحلم العلماء بالآلة تقتصر الأمر على الأمان ولكنهم يحلمون أن تستخدم التكنولوجيا كوسيلة للراحة أيضاً، فيحل الإصبع محل المفاتيح الكثيرة المتعبة التي يحملها الشخص في كل مكان أو البطاقات التي تفتقد بعضها ببعض والمعرضة لأن تفقد، وتعرض صاحبها للسرقة.

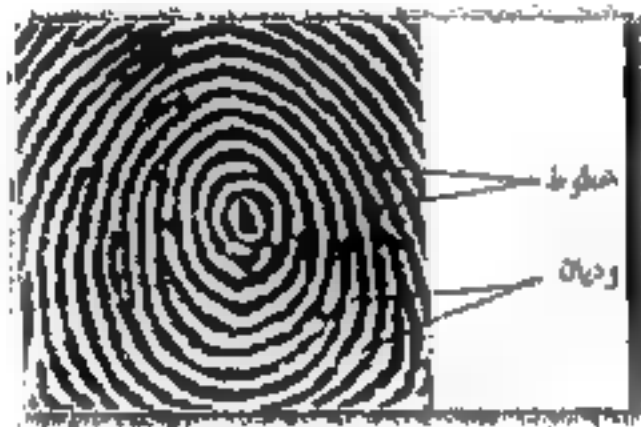
ويأمل العلماء أيضاً أن يكون الإصبع هو الوسيلة للدخول إلى المنزل أو محل العمل أو فتح بوابة جراج المنزل والمصعد وجهاز الكمبيوتر، هذا بالإضافة إلى توفير المزيد من الضمان عند سحب الأموال من ماكينات البنوك في الشوارع.

وللبصمة شكل مميز لكل شخص، وهي تتكون قبل الولادة وتحتفظ بهذا الشكل المميز طوال فترة الحياة، وتتعرض للعديد من العوامل مثل السن، تأثير طبيعة العمل اليدوي،

الجروح، إلا أن الصفات المميزة لها تبقى موجودة، وتتمتع بمزايا تفضيلية مقارنة مع المحددات البيومترية الأخرى كسهولة الاستخدام، سرعة التصنيف، انخفاض كلفة التسجيل، إمكانية إيجاد البصمة في مكان الجرائم.

تصنيف البصمة :

البصمة عبارة عن شكل مؤلف من مجموعة من الخطوط البارزة وفراغات بين هذه الخطوط تسمى بالأخاديد (أو الوديان)، وهي مجموعة من الخطوط والأخاديد والتي لها شكل مميز خاص بكل شخص تتم عملية التأكد من الهوية أو التعرف عليها^(١).



شكل رقم (٢-٥) يوضح البصمة

وتصنيف البصمة هو عبارة عن تقنية تمكن من تحديد النوع الذي تنتمي إليه البصمة ضمن عدة أنواع محددة مسبقاً، مما يؤدي إلى مقارنة الدخّل مع مجموعة فرعية من البصمات في قاعدة بيانات أنظمة التعرف على البصمة، والعمل على اختصار زمن البحث ودرجة تعقيد الحساب في هذه الأنظمة تشمل الأنواع الرئيسية لتصنيف البصمة خمس فئات وهي ما يلي:

(١) هويدا مصري عبد النبي، سيد تافع : تطوير نظام آلي للتعرف على بصمة الإصبع، رسالة ماجستير، جامعة حلوان، الحاسبات والمعلومات، علوم اتحاسب، القاهرة، ٢٠٠٥.

أ- الحلقة اليسارية:

حيث يدخل خط واحد أو أكثر من خطوط البصمة من الجهة اليسارية، ثم يتقوس إلى الخلف ويخرج من الجهة نفسها التي دخل منها.



شكل رقم (٢-٥) يوضح الحلقة اليسارية

ب- الحلقة اليمينية:

وهي مماثلة للحلقة اليسارية باستثناء كون خطوط البصمة تدخل وتخرج من الجهة اليمينية.



شكل رقم (٤-٥) يوضح الحلقة اليمينية

ج- النوع الحلزوني:

حيث تحتوي البصمة على الأقل على خط واحد من خطوط البصمة والذي يشكل مساراً كاملاً ٣٦٠ درجة (دائرة كاملة) حول مركز البصمة. ويمكن أن توجد في هذا الصنف من البصمات حلقتان (أو حلزون واحد)، وهذا الصنف معقد جداً، وأحياناً يقسم إلى فئتين: الحلزون المنبسط والحلقة التوأم أو الحلقة المزدوجة.



شكل رقم (٥-٥) يوضح النموذج الحلزوني

د- القوس (القوس المنبسط):

حيث تدخل خطوط البصمة من جانب ما وتتجه إلى الجانب الآخر مع ارتفاع و تموج في الوسط.



شكل رقم (٥-٦) يوضح القوس المنبسط

هـ- القوس على شكل خيمة:

وهو مماثل للنوع آنف الذكر، باستثناء وجود قوس على لخط واحد من خطوط البصمة على الأقل.



شكل رقم (٧-٥) يوضح القوس على شكل خيمة

تصميم وتنفيذ النظام :

تتمحور النقاط الأساسية لتصميم نظام التعرف الآلى على البصمة حول اختيار طريقة عمل النظام («تأكد من الهوية، أو تحديد الهوية»)، واختيار مكونات الكيانات الصلب واللين وجعلها يعملان معاً، ويفضل طريقة «التأكد من البصمة» عندما يكون عدد المستخدمين كبيراً، علماً بأن النظام المعتمد على طريقة «تحديد الهوية» هو أكثر صمودية فى التصميم بسبب الوضع الحرج لمسألتي السرعة والدقة. وفى حال تصميم نظام يعتمد على بعض المكونات الجاهزة، فعلى مصمم النظام مراعاة مجموعة من العوامل عند انتقائه لهذه المكونات، مثل التقنية المستخدمة، ومدى توافق مواصفات هذه المكونات مع المتطلبات المحددة للمنتج النهائي، وتوافق البرمجيات مع منصة التشغيل، مع مراعاة التناقض بين الكلفة والأداء، وهو مرتبط بمتطلبات التطبيق، وتوفر الوثائق والدعم المناسبين من الجهات المنتجة لهذه المكونات.

ويتم التقاط صورة البصمة عن طريق الماسح الضوئي، ويتم إدخالها إلى وحدة التعرف؛ حيث تتم معالجة الإشارة الناتجة عن البصمة، ويتم استخلاص السمات الأساسية لها، وتحويلها إلى قيم رقمية خاصة بالبصمة المدخلة، وهذا يتم التمييز بين حالتين:

حالة التسجيل:

حيث تدخل البصمة إلى النظام لأول مرة وتقرن برقم شخصي خاص يستخدم النظام ويتم إدخاله بواسطة لوحة الملامس، وفي هذه الحالة فإن سمات البصمة تخزن على شكل «قالب» في قاعدة البيانات الموجودة ضمن وحدة التعرف، ويستخدم هذا القالب للمقارنة في كل مرة يتم وضع البصمة ذاتها على الماسح وإدخال الرقم الشخصي المرتبط بها والمخزن في قاعدة البيانات.

حالة استخدام النظام:

حيث يقوم المستخدم بإدخال البصمة المخزن قالبها وذلك بواسطة الماسح الضوئي، وإدخال رقمه الشخصي - أيضاً - بواسطة لوحة الملامس، وعندئذ تقوم وحدة التعرف باستخلاص السمات العائدة لهذه البصمة ومقارنتها مع القالب العائد للرقم الشخصي ذاته، وهنا يتم التمييز بين حالتين:

- حصول التطابق:

في حالة حدوث تطابق فإن النظام يقبل المستخدم، سواء كان في حالة دخول أو خروج للمؤسسة، ويتم بيان ذلك بواسطة مؤشر ضوئي وتشكيل إشارة التحكم المناسبة، وإثبات توقيت العملية سواء كانت دخول أو خروج.

- عدم حصول التطابق :

وعندئذ فإن النظام لا يقبل المستخدم، ويتم بيان ذلك بواسطة مؤشر ضوئي أيضاً وإشعار مدير النظام بهذه النتيجة، وإخطاره بأن هناك محاولة دخول غير شرعية. وفي كلتا الحالتين يتم تسجيل بيانات المستخدم في قاعدة البيانات، وذلك لتوثيق هذه البيانات من جهة، ولإعداد التقارير المختلفة (اليومية، الأسبوعية، الشهرية) عن موظفي المؤسسة المستخدمة.

ثالثاً - البصمة الوراثية :

لم تُعرّف البصمة الوراثية حتى كان عام ١٩٨٤، حينما نُشر «د. أليك جيفريز» عالم الوراثة بجامعة «ليستر» بلندن بحثاً أوضح فيه أن المادة الوراثية قد تتكرر عدة مرات، وتعيد نفسها في تتابعات عشوائية غير مفهومة، وواصل أبحاثه حتى توصل بعد عام واحد إلى أن هذه التتابعات مميزة لكل فرد، ولا يمكن أن تتشابه بين اثنين إلا في حالات التوائم المتماثلة فقط؛ بل إن احتمال تشابه بصمتين وراثيتين بين شخص وآخر هو واحد في التريليون، مما يجعل التشابه مستحيلاً؛ لأن سكان الأرض لا يتعدون المليارات الستة، وسجل الدكتور «أليك» براءة اكتشافه عام ١٩٨٥، وأطلق على هذه التتابعات اسم «البصمة الوراثية للإنسان» *The DNA Fingerprint*، وعرّفت على أنها «وسيلة من وسائل التعرف على الشخص عن طريق مقارنة مقاطع (DNA)»، وتُسمى في بعض الأحيان الطبعة الوراثية «DNA Typing»^(١).

ولم تتوقف أبحاث «د. أليك» على هذه التقنية؛ بل قام بدراسة على إحدى المائات يختبر فيها توريث هذه البصمة، وتبين له أن الأبناء يحملون خطوطاً يجيء نصفها من

(1) Henry C. Lee, R.E. Gaensslen : *Advances in Fingerprint Technology*, 2nd ed, Boca Raton, Fla. : CRC Press, c2001, p 34.

الفصل الخامس - دور التقنيات الحديثة في تطوير تكنولوجيا المعلومات الحديثة

الأم، والنصف الآخر من الأب، وهي مع بساطتها تختلف من شخص لآخر. ويكفى لاختبار البصمة الوراثية نقطة دم صغيرة؛ بل إن شعرة واحدة إذا سقطت من جسم الشخص المراد، أو ألعاب مال من فمه، أو أى شيء من لوازمه، فإن هذا كفىل بأن يوضح اختبار البصمة بوضوح.

وقد تمسح إذا بصمة الأصابع بسهولة، ولكن بصمة الـ «(DNA)» يستحيل مسحها، وبمجرد المصافحة قد تنقل الـ «(DNA)» الخاصة بالشخص إلى يد من يصافحه، والبصمة الوراثية لا تتغير من مكان لآخر في جسم الإنسان، فهي ثابتة بغض النظر عن نوع النسيج، فالبصمة الوراثية التي في العين تجد مثيلاتها في الكبد، والقلب، والشعر.

تعريف البصمة الوراثية:

البصمة الوراثية عبارة عن عملية عزل للحمض النووي (DNA) عن مصادره الحيوية بواسطة إنزيمات خاصة تقسم هذا الحمض إلى مواقع قيد؛ حيث يكون له تسلسل معين، ومن ثم يتم تصنيف أجزاء الحمض النووي التي يتم الحصول عليها بهذه الطريقة بواسطة الأجهزة الكهربائية التي تتمثل في أن يوضع المخطول الذي يحمل أجزاء الحمض النووي تحت مجال كهربائي، وبطريق خاصة يتم جعلها مرئية ويتم التمييز بين الأجزاء ووضع علامات على كل منها يمكن أن تظهر منه الركيزة (التصوير الإشعاعي الذاتي) وذلك يترك خطوط واضحة إلى حد ما والمقارنة من حيث العدد والمكان الخاص بصورتين إشعاعيتين يتيح الوصول إلى هوية مصدرها البيولوجي^(١)، والحمض النووي عبارة عن مادة كيميائية تتحكم في تطوير شكل الخلايا والأنسجة في جسم الإنسان، فهو بمثابة خريطة خاصة بتطوير الجسم محفوظة في داخل كل خلية من خلاياه.

(١) جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، القاهرة، دار النهضة العربية للطبع والنشر والتوزيع، ٢٠٠٢م، ص ٥٩.

والحمض النووي يختصر بالأحرف (DNA) وهي الحروف الأولى لمصطلح (Deoxy Nevulice Acid) أي الحمض النووي وهي أيضاً عبارة عن مركب كيميائي معقد ذو وزن جزئي عالٍ لا يمكن للكائن الحي الاستغناء عنه يعرف (DNA) وهي اختصار لكلمة الحمض النووي الديوكسي منزوع الأكسجين والحمض النووي هو الذي يحمل المعلومات الوراثية ويكوّن من خطين دائريين (النيوكليوتيدات) على شكل حلزون ويوجد هذا الحمض في أنوية الخلايا للكائنات الحية لذا يطلق عليه (الحمض النووي) وترجع أهمية الحمض النووي إلى أن الـ (DNA) في الخلية يشمل جميع الكروموسومات بداخل نواة الخلية وتشكل الكروموسومات نظاماً، وهذا النظام أو الترتيب هو الذي يحدد خصائص كل فرد باعتباره أنها تختلف من شخص لآخر.

التعريف الاصطلاحي للبصمة الوراثية :

اجتهد العلماء المعاصرون في وضع تعريف للبصمة الوراثية إلا أن تعريفاتهم تباينت، فهناك من عرفها بأنها «تعيين هوية الإنسان عن طريق تحليل جزء أو أجزاء من حمض (DNA) المتمركز في نواة أية خلية من خلايا جسمه»، ورأي آخر يرى أنها «المادة الحاملة للعوامل الوراثية والجينات في الكائنات الحية»^(١)، ورأي يرى أنها «صورة لتركيب المادة الحاملة للعوامل الوراثية أي هي صورة الحمض النووي (DNA) الذي يحتوي على الصفات الوراثية للإنسان أو بمعنى أدق هي صورة تابع النيوكليوتيدات التي تكون جزء الحمض النووي الوراثي DNA، وتمتد وسيلة من وسائل التعرف على الشخص عن طريق مقارنة مقاطع الـ (DNA)».

ونميل إلى الرأي الذي يرى أن البصمة الوراثية هي «تعيين هوية الإنسان عن طريق تحليل جزء أو أجزاء من الحمض النووي المتمركز في نواة أية خلية من خلايا جسمه».

(١) طارق إبراهيم الدسوقي، عطية : البصمات وأثرها في «الإثبات الجنائي»، دار الجامعة الجديدة، الإسكندرية، ٢٠١١م، ص ٥١.

حيث إن تلك المادة حاملة للعوامل الوراثية والجينات في الكائنات الحية بالفواة.

مجالات العمل بالبصمة الوراثية :

يرى المختصون وخبراء البصمات أنه يمكن استخدام البصمات الوراثية في مجالات كثيرة، ترجع في مجملها إلى مجالين رئيسيين، هما:

١ - المجال الجنائي:

وهو مجال واسع يدخل ضمنه الكشف عن هوية المجرمين في حالة ارتكاب جريمة قتل، أو اعتداء، وفي حالات الاختطاف بأنواعها، وفي حالة انتحال شخصيات الآخرين ونحو هذه المجالات الجنائية^(١).

٢ - مجال النسب :

وذلك في حالة الحاجة إلى إثبات البنوة أو الأبوة لشخص، أو نفيه عنه، وفي حالة اتهام المرأة بالحمل من وطء شبهة، أو زنا.

خصائص البصمة الوراثية:

١- تتمتع البصمة الوراثية بميزة الدقة، وتعتبر أدق وسيلة عُرفت حتى الآن في تحديد هوية الإنسان، وذلك لأن نتائجها قطعية لا تقبل الشك، وإحدى المشاكل التي لم تجد حلاً في الطرق التقليدية هي فحص المادة الجسدية المختلطة مثل الحيوانات المنوية المختلطة بالإفرازات المهبلية، أما بالنسبة لاختبار الحمض النووي فلا يُشكل مثل هذا الاختلاط أية مشكلة في الكشف عن تركيب هذا الحمض، ولذلك أهميته في قضايا القتل الجنسي بصفة خاصة بحيث تختلط الحيوانات المنوية للجاني بالإفرازات المهبلية للمجنى عليها.

(١) محمد أحمد غانم : الوراثية الجنائية والشرعية للإثبات الجنائي بالشفرة الوراثية، القاهرة ، بدون ناشر، ص ٦١.

٢- يعتبر تحليل الـ (DNA) (البصمة الوراثية)، وسيلة فعّالة في مجال البحث عن الحقيقة من حيث إثبات الجريمة أو نقيها بدقة تامة؛ حيث توجد في كل خلية في جسم الإنسان بطاقة لا يمكن تزويرها فيمكن مقارنة منطقة الحمض النووي الذي يعتمد عليه في مكان وقوع الجريمة بمنطقة الحمض النووي للمادة أو الخلية المأخوذة من المتهم، ووجود منطقتين متطابقتين يعتبر دليلاً شبه مطلق على أن الخلية هي للشخص نفسه، فيما عدا حالة وجود توأم أحادي البويضة حيث لا يمكن الجزم بذلك.

٣- البصمة الوراثية التي يحملها الحمض النووي شديدة المقاومة ولا تتأثر بالظروف الجوية من حرارة، ورطوبة، وجفاف، ولا تتلف وتقاوم عوامل التحلل والتعفن، ويمكن حفظها واستخدامها لعدة سنوات فيمكن عمل البصمة من الآثار الحديثة والقديمة جداً.

٤- أن تركيب جزئي الحمض النووي لا يختلف من خلية لأخرى، فالحمض النووي في أية خلية دموية يطابق تماماً الحمض الموجود في أية مادة حيوية، بمعنى أن الحمض النووي لدى الأفراد متطابق في كل خلايا الجسم ولا يتغير أثناء الحياة^(١).

٥- عدم إمكانية الخلط بين جزئين متواجدين في مسرح الجريمة ولكن لشخصين مختلفين؛ حيث يمكن الفصل بينهما مهما كان الحال من الاختلاط، فيسهل فيها الفرز.

٦- للبصمة الوراثية الميزة الفنية التي تقطع الشك باليقين، تعتبر دليل نفي وإثبات قاطع بنسبة ١٠٠ ٪، وذلك لأن احتمال التشابه بين البشر في الـ (DNA) غير

(١) رمسيس بهنام، البروفيسور العالمي وفن التحقيق، منشأة المعارف بالإسكندرية ١٩٩٦م، ص ٢٠.

وارد، يعكس فصائل الدم، التي تعتبر وسيلة نفى فقط لاحتمال التشابه بين البشر في هذه الفصائل.

٧- يمكن التوصل للبصمة الوراثية لأي شخص بالبحث والفحص الدقيق للحمض النووي، من أية مخلفات آدمية سائلة (دم، منى، لعاب) أو أنسجة (لحم، عظم، شعر) وهذه ميزة مهمة في حالة عدم العثور على بصمات أصابع المجرم.

٨- البصمة الوراثية (DNA) توجد في أنوية جميع الخلايا باستثناء كرات الدم الحمراء؛ حيث لا يوجد فيها نواة، ولذلك يمكن استخراج سائل النواة الـ (DNA) بسهولة من جذور الشعر وكرات الدم البيضاء والعظام وإفرازات الإنسان كالمني واللُعاب والفضلات، وبذلك يمكن مقارنة المادة الحيوية لإحدى الخلايا مثل الخلية الدموية، بمادة أخرى مثل الغشاء المخاطي لغدة الفم، وقد أثبتت التجارب والاختبارات أن لكل مخلوق (DNA) منفرد في الشكل والطول والمميزات ومواقع الترسيب ما عدا التوائم الذي يأتي من بويضة واحدة.

٩- على أثر نجاح البصمة الوراثية وما تتمتع به من خصائص ومميزات، والمكانة التي تستعدى أن يستعان بها الخبراء، وإمكانية تحديد هوية الأشخاص، كما أنها من أدق الوسائل للتوصل إلى الفاعل الحقيقي بأسرع الطرق، وذلك اعتمد مكتب التحقيقات الفيدرالية بالولايات المتحدة الأمريكية طريقة اختبار سائل نواة الخلية (DNA) كأحدى الوسائل المعتمدة في إجراءات البحث الجنائي.

١٠- تظهر بصمة الحمض النووي على هيئة خطوط عرضية يسهل قراءتها وحفظها وتخزينها في الكمبيوتر لحين الطلب للمقارنة، يعكس بصمات الأصابع، التي لا يمكن حفظها في الكمبيوتر، شرعت بعض الدول بتأسيس بنك لقاعدة بيانات الحمض النووي لكافة مواطنيها، ودول أخرى اقتصرت على المشتبه

فيهم، كي يكون لديها دليل في حالة الاشتباه وفي حالة الاختفاء.

١١- أهم مميزات البصمة الوراثية في تعرّد كل شخص بها على حدة دون خلط مما يساعد على جلاء الحق وإزالة أية شوائب تشبه بل والتثبت على اليقين دون الشك وذلك فيما عدا حالة التوائم المتشابهة، ويمكن الحصول عليها من أي من أجزاء الجسم حتى في حالة التعفن.



قائمة المراجع

قائمة المراجع

أولاً- الكتب :

- أحمد سيد مصطفى : إدارة الإنتاج والعمليات في الصناعة والخدمات، مكتبة الأنجلو المصرية، الطبعة الثالثة، القاهرة، ١٩٩٧ م.
- المدير العربي في عالم متغير، القاهرة، بدون ناشر، القاهرة، ٢٠٠٢ م.
- إسماعيل محمد السيد : نظم المعلومات لاتخاذ القرارات الإدارية، الإسكندرية، المكتب العربي الحديث للطباعة والنشر، ٢٠٠١ م.
- أشرف السعيد أحمد : تكنولوجيا المعلومات وإدارة الأزمات، القاهرة، ٢٠١٢ م.
- أثر تكنولوجيا الأزمات على إدارة الأزمة الأمنية (دراسة تطبيقية)، القاهرة، ٢٠١١ م.
- القرصنة الإلكترونية، القاهرة، ٢٠١٢ م.
- مقدمة في علوم الحاسب، القاهرة، ٢٠١١ م.
- جميل عبد الباقي : أدلة الإصابات الجنائية والتكنولوجيا الحديثة، القاهرة، دار النهضة العربية، ٢٠٠٢ م.
- حسن علي الزغبى : نظم المعلومات الاستراتيجية، عمان، دار وائل للنشر والتوزيع، الطبعة الأولى، ٢٠٠٥ م.
- حسن عماد مكاوي : تكنولوجيا الاتصال الحديثة في عصر المعلومات، الطبعة الأولى، القاهرة، الدار المصرية اللبنانية، ١٩٩٣ م.

حسني المحمدي بواوي ، الوسائل العلمية الحديثة في الإثبات الجنائي،
الإسكندرية، منشأة المعارف، ٢٠٠٥م.

خالد ممدوح إبراهيم : أمن الحكومة الإلكترونية، الإسكندرية، الدار الجامعية،
٢٠٠٨م.

رأفت رضوان : الحكومة الإلكترونية، القاهرة، المركز الدولي للدراسات
المستقبلية والإستراتيجية، ٢٠٠٥م.

رمسيس بهنام ، البوثيس العلمي وفن التحقيق، منشأة المعارف
بالإسكندرية ١٩٩٦م.

طارق إبراهيم الدسوقي ، البصمات وأثرها في الإثبات الجنائي، دار الجامعة
الجديدة، الإسكندرية، ٢٠١١م.

- الأمن المعلوماتي، النظام القانوني لحماية المعلومات،
القاهرة، دار الجامعة الجديدة، ٢٠٠٩م.

طارق طــــه ، نظم المعلومات والحاسبات الآلية من منظور إداري،
القاهرة، دار الفكر العربي، ٢٠٠٨م.

عبد الحكيم أحمد الخزامي : فن اتخاذ القرار مدخل تطبيقي، مكتبة ابن سينا ، القاهرة،
١٩٩٩م.

عصمت عبد الله الشيخ : دور نظم وتكنولوجيا المعلومات في تيسير وفاعلية
العمل الإداري، دار النهضة العربية، ١٩٩٨م.

علاء عبد الرازق السالى : نظم إدارة المعلومات، النوحة - قطر، المنظمة العربية للتنمية الإدارية، ٢٠٠٢م.

على عبد الهادى مسلم : مذكرات فى نظم المعلومات المبتية على الكمبيوتر- المبادئ والتطبيقات، مركز التنمية الإدارية، جامعة الإسكندرية، ١٩٩٤م.

على فهمى : نظم دعم اتخاذ القرار والأنظمة الذكية، القاهرة، دار الكتب للنشر والتوزيع، القاهرة، ٢٠٠٤م.

عماد عبد الوهاب الصباغ : علم المعلومات، دار الثقافة للنشر والتوزيع ، قطر، ٢٠٠٤م.

فريد النجار : الحكومة الإلكترونية، بين النظرية والتطبيق، الإسكندرية، الدار الجامعية، ٢٠٠٨م.

محمد أحمد ضائم : الجوانب القانونية والشرعية للإثبات الجنائى بالشفرة الوراثية، القاهرة، ٢٠٠٧م.

محمد السعيد خشبة : نظم المعلومات المفاهيم والتكنولوجيا، دار الإشعاع للطباعة، القاهرة، ١٩٨٧م.

محمد محمد الهادى : التطورات الحديثة لنظم المعلومات المبتية على الكمبيوتر، القاهرة، دار الشروق، ١٩٩٢م.

ثانياً - الأبحاث والدراسات:

أحمد سيد مصطفى : انعكاسات التكنولوجيا على العنصر البشري في المنظمات العربية، ورقة عمل نشرت بمجلة آفاق اقتصادية، العدد ٧٣، مجلد ١٩، ١٩٨٩ م.

هويدا يسري عبدالنبي سيدنافع : تطوير نظام آلي للتعرف على بصمة الإصبع، رسالة ماجستير، جامعة حلوان، الحاسبات والمعلومات، علوم الحاسب، القاهرة، ٢٠٠٩ م.

يونس صرب : الخصوصية وأمن المعلومات، ورقة عمل مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخليوي - اتحاد المصارف العربية، ٢٠ - ٢٢ أيار ٢٠٠١، عمان - الأردن، ٢٠٠١ م.

ثالثاً - الندوات :

ندوة تكنولوجيا المعلومات الأمنية، سنوات من التحديث والإنجاز مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة، ٢٠٠٤ م.

رابعاً - الكتب والمراجع الأجنبية:

Bhunia, C.T : Information Technology Network, New AGE, 2005

Collin, S. M. H : Dictionary of Information Technology, London: Peter Collin Pub, 1996.

E.Wainright Martin : Managing Information Technology : What Managers Need To Know? (New Jersey : Prentice Hall), 1999.

- Fletcher, Keith** : **Marketing Management And Information Technology**,
New York: Prentice Hall, 1995.
- Gershenfeld, N** : **The Physics Of Information Technology** ,Cambridge;
New York : Cambridge University Press ,2000.
- Henry C. Lee, R.E** : **Gaensslen, Advances in Fingerprint Technology**, 2nd
ed, Boca Raton, Fla. : CRC Press, c2001.
- Henry C. Lee, R.E** : **Advances in Fingerprint Technology**, 2nd ed, Boca
Gaensslen. Raton, Fla. : CRC Press, c2001.
- Horrington Jon** : **Organization Structure And Information Technology**,
New York Prentice Hall International , 1991.
- Indira Carr** : **Computer Crime International Library of Criminology**,
Criminal Justice and Penology - Second Series Ashgate,
C2009.
- K. Samuelson and H: Information System And Network Amsterdam** :
Borko and G.X.Aney. North Holand Publishing Co.,)1977.
- Karl De Leeuw, J: The History of Information Security: A Comprehensive**
A. Bergstra. Handbook, Elsevier, 2007.
- Kimberly Kiefer** : **Information Security: A Legal, Business, and**
Technical Handbook, American Bar Association,
C2004
- L. Jean Camp, Stephen** : **Economics of Information Security**, Springer, C2004.
Lewis.



- L.C. Jain** : **Intelligent biometric techniques in fingerprint and face recognition**, Boca Raton: CRC Press, C1999
- Lucas, Henry C** : **Information Technology For Management -7 th ed** (Boston :Irwin /McGraw -Hill), 2000.
- Nalini Ratha, Ruud** : **Automatic Fingerprint Recognition Systems**, New York: Springer, c2004.
- O'Brien ,James A** : **Management Information Systems :3rd ed** ,Chicago: Irwin, 1996.
- ohn R. Vacca** : **Computer and Information Security Handbook**, Morgan Kaufmann, C2009.
- Oliver. E.C. ; Chapman,** : **Data processing And Information Technology -8 ed**, R.J. French, C.S. DP Publications, Reviser, 1990.
- Owen, Jo** : **The leadership skills handbook**, London; Philadelphia: Kogan Page,2006.
- Paulus R. Wayleith** : **Data Security: Laws and Safeguards**, Nova Science Publishers, C2008.
- Rosenthal, Uriel,** : **Crisis Management and Decision Making**, Dordrecht, Pijnenburg, Bert. Boston :Kluwer Academic Publishers,1991.
- Tyler Moore** : **Economics of Information Security and Privacy**, Springer, C2010.

Weisman, H.M : Information Systems Services And Centers. London:
John Wiley, 1972.

Williams, Brian K, : Using Information Technology, 4 th ed, Boston:
Sawyer, Stacey C. : McGraw - Hill, 2001.

Yadav, D.S : Foundations Of Information Technology-3 rd ed, New
age international limited publishers, 2006.

خامساً - مواقع الإنترنت:

- www.egypt.gov.eg



فهرس الموضوعات

الفهرس

الموضوع	الصفحة
الفصل الأول : تكنولوجيا المعلومات	٩
أولاً : ماهية التكنولوجيا وخصائصها	١٢
ثانياً : مفهوم المعلومات	١٥
مصادر المعلومات :	١٥
ثالثاً : مفهوم تكنولوجيا المعلومات	٢٠
رابعاً : أنواع نظم المعلومات	٢٣
الفصل الثاني : تكنولوجيا المعلومات الأمنية	٢٧
أولاً : نشأة نظام المعلومات في وزارة الداخلية	٣٠
ثانياً : التخطيط الاستراتيجي لتطوير نظم المعلومات وزارة الداخلية	٣٢
ثالثاً : مقومات بناء تكنولوجيا المعلومات الأمنية	٣٣
رابعاً : أهداف تكنولوجيا المعلومات الأمنية	٣٧
خامساً : خصائص ومميزات المعلومات الأمنية	٣٨
سادساً : معايير جودة المعلومات الأمنية	٤١
سابعاً : تكنولوجيا المعلومات وصنع القرار الأمني	٤٦
ثامناً : مدى الحاجة لتكنولوجيا المعلومات في العمل الأمني	٥٢
الفصل الثالث : استراتيجية أمن المعلومات	٥٥
أولاً : مفهوم أمن المعلومات	٥٨
ثانياً : مفهوم الاستراتيجية	٦١
ثالثاً : محل الحماية	٦٦

٦٨	رابعاً : المخاطر المحتملة
٧٢	خامساً : أهم أساليب تأمين قواعد البيانات
٨٧	الفصل الرابع : تكنولوجيا المعلومات الأمنية والحكومة الإلكترونية
٩٠	أولاً : مفهوم الحكومة الإلكترونية
٩٣	ثانياً : مشروعات وزارة الداخلية المصرية في مجال الحكومة الإلكترونية
	ثالثاً : تكنولوجيا المعلومات الأمنية في مجال تيسير وتبسيط إجراءات
١٠١	حصول المواطنين على الخدمات الأمنية الجماهيرية
	الفصل الخامس : دور التقنيات الحديثة في تطوير تكنولوجيا
١١٩	المعلومات الأمنية
١٢٢	أولاً : مفهوم التقنية البيومترية
١٣٠	ثانياً : بصمة الإصبع
١٣٧	ثالثاً : البصمة الوراثية
١٤٥	قائمة المراجع
١٥٥	فهرس الموضوعات

دار الكتاب الحديث :

- العنوان : ٩٤ ش عباس العقاد - مدينة نصر - القاهرة

- تليفون : ٢٢٧٥٢٩٩٥ - ٢٢٧٥٢٩٩٣

المجموعة العربية للاستشارات والتدريب والنشر :

- العنوان : ٨ ش أحمد فخرى - مدينة نصر - القاهرة

- تليفون : ٢٢٧٣٩١١٠

دار العلوم للنشر والتوزيع :

- العنوان : ٢٩ ش ١ - مكتبات المعادى - القاهرة

- تليفون : ٢٣٥٩٣٩١٨

دار الفكر العربى :

- العنوان : ٩٤ شارع عباس العقاد - مدينة نصر - القاهرة

- تليفون : ٢٢٧٥٢٩٨٤

- العنوان : ١٦ شارع جواد حسنى - القاهرة

- تليفون : ٢٣٩٣٠١٦٧

دار النهضة العربية :

- العنوان : ٣٢ ش عبدالخالق ثروت - القاهرة

- تليفون : ٢٣٩٢٦٩٣١

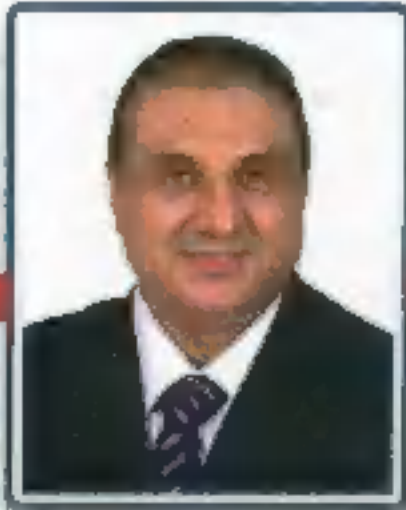


للكميات : ASHRAF.M3R62@GMAIL.COM

Inv:2975

Date:20/4/2014

.....



تكنولوجيا المعلومات في المجال الأمني

يتناول هذا الكتاب دور المعلومات في قطاع البشر، حيث أصبح يقاس التقدم في أية مهنة أو منظمة أو دولة بما يتوافر لدى أي منهم من مستودع من المعلومات، ولقد أثر التطور السريع

لتكنولوجيا المعلومات تأثيراً كبيراً وبالفعل في واقع العمل الأمني، وكان لوزارة الداخلية الحرص على مواكبة التقدم التكنولوجي وتوظيف تكنولوجيا المعلومات لخدمة الأغراض الأمنية، والتحول من الإدارة التقليدية إلى الإدارة الإلكترونية لتصبح من الركائز الأساسية لنجاح الحكومة الإلكترونية في مصر، بما يضمن الارتقاء بمستوى أداء الأجهزة الشرطية، باستخدام التقنيات المعلوماتية الحديثة، وقد تناولنا الموضوع من خلال خمسة فصول: الفصل الأول بعنوان تكنولوجيا المعلومات، ونعرض من خلاله ماهية التكنولوجيا وخصائصها، ومفهوم وأنواع نظم المعلومات، والفصل الثاني بعنوان تكنولوجيا المعلومات الأمنية، وتناولنا من خلاله نشأة نظام المعلومات، والتخطيط الاستراتيجي لتطوير نظم المعلومات بوزارة الداخلية، وأهداف وخصائص تكنولوجيا المعلومات الأمنية، ومدى الحاجة لتكنولوجيا المعلومات في العمل الأمني، والفصل الثالث بعنوان استراتيجية أمن المعلومات، وتناولنا من خلاله مفهوم أمن المعلومات، ومفهوم الاستراتيجية، وأهم أساليب تأمين قواعد البيانات، والفصل الرابع بعنوان تكنولوجيا المعلومات الأمنية والحكومة الإلكترونية، وتناولنا من خلاله مفهوم الحكومة الإلكترونية، وتطبيقات وزارة الداخلية المصرية في مجال الحكومة الإلكترونية، والفصل الخامس بعنوان دور التقنيات الحديثة في تطوير تكنولوجيا المعلومات الأمنية، مفهوم التقنية البيومترية، وبصمة الإصبع، البصمة الوراثية. وندعو الله أن تكون قد وفقنا في المساهمة ولو بشكل بسيط في عرض المعلومات الأساسية، التي تساعد الباحثين والمهتمين بمجال تكنولوجيا المعلومات الأمنية لهامة عصر تكنولوجيا المعلومات.



من الإصدارات السابقة

يطلب من المكتبات التالية:

دار الفكر العربي - دار العلوم للنشر والتوزيع - دار النهضة العربية
دار الكتاب الحديث - المجموعة العربية للاستشارات والتدريب والنشر